ARTICLE IN PRESS

Ad Hoc Networks xxx (2013) xxx–xxx

Contents lists available at SciVerse ScienceDirect

Ad Hoc Networks

journal homepage: www.elsevier.com/locate/adhoc

TC-BAC: A trust and centrality degree based access control model in wireless sensor networks

Junqi Duan [a], Deyun Gao [a,*], Chuan Heng Foh [b], Hongke Zhang [a]

[a] School of Electronic and Information Engineering, Beijing Jiaotong University, Beijing 100044, PR China
[b] Center for Communication Systems Research, University of Surrey, Guildford , Surrey, GU2 7XH, United Kingdom

ARTICLE INFO

Article history:
Available online xxxx

Keywords:
Access control
Trust computation
Centrality degree
Wireless sensor networks

ABSTRACT

Access control is one of the major security concerns for wireless sensor networks. However, applying conventional access control models that rely on the central Certificate Authority and sophisticated cryptographic algorithms to wireless sensor networks poses new challenges as wireless sensor networks are highly distributed and resource-constrained. In this paper, a distributed and fine-grained access control model based on the trust and centrality degree is proposed (TC-BAC). Our design uses the combination of trust and risk to grant access control. To meet the security requirements of an access control system with the absence of Certificate Authority, a distributed trust mechanism is developed to allow access of a trusted node to a network. Then, centrality degree is used to assess the risk factor of a node and award the access, which can reduce the risk ratio of the access control scheme and provide a certain protection level. Finally, our design also takes multi-domain access control into account and solves this problem by utilizing a mapping mechanism and group access policies. We show with simulation that TC-BAC can achieve both the intended level of security and high efficiency suitable for wireless sensor networks.

1. Introduction

Wireless sensor networks (WSNs) typically consist of a large number of resource-constrained nodes deployed in an unattended area. The low-cost and low-power sensor nodes have the ability to cooperatively perceive characteristics of the physical world, such as temperature, sound, vibration and pressure without manual operation [1,2]. Owing to these characteristics, many feasible applications have been proposed, including intelligent buildings, health monitoring, battlefield surveillance, space exploration [3,4].

However, deployment in a highly distributed manner in an open and remote environment also gives rise to security threats in WSNs. A remote environment prevents an administrator from physically examining the network. As a result, foreign nodes may be introduced. Additionally, sensor nodes use a wireless broadcast channel to communicate, which introduces openness in communications in a local region. Moreover, end-to-end communication in a WSN is achieved using multi-hop communication where a communication path is usually established in a distributed manner. All these operations in a WSN give an opportunity to a foreign node to be physically present in a WSN without detection, or even a legitimate node to be physically compromised without notice. Then, the foreign or compromised node may intercept or hijack a communication to launch an attack on other nodes [5–7]. While solutions exist and have been successfully demonstrated in other types of networks [8,9], it is unfortunate that many practical security mechanisms are too complicated to be practically implemented in a WSN as it is a resource-constrained system in terms of bandwidth, memory, and computing power.

* Corresponding author.
E-mail address: gdeyun@gmail.com (D. Gao).

1570-8705/$ - see front matter © 2013 Elsevier B.V. All rights reserved.
http://dx.doi.org/10.1016/j.adhoc.2013.05.005

Please cite this article in press as: J. Duan et al., TC-BAC: A trust and centrality degree based access control model in wireless sensor networks, Ad Hoc Netw. (2013), http://dx.doi.org/10.1016/j.adhoc.2013.05.005

Granting proper access to legitimate nodes is essential to ensure correct operation of WSNs. Access control in WSNs can be defined as the process of limiting access to sensitive information only to trusted nodes or other systems in a WSN. A proper design of an access control ensures that information is accessible only to any authorized and trustworthy node. In other words, foreign nodes that are not authorized or compromised nodes that have unusual behavior should be prevented from accessing sensitive information.

Different models of access control have been proposed over the years [10–12]. However, most access control models were developed for some specific systems not suitable for a resource-constrained system such as a WSN. Certain supports are required for the access control that targets WSNs. In the following, we summarize the unique challenges of WSNs to support a proper access control:

- *Remote deployment*: WSNs are often deployed in a remote and open environment. It is difficult to prevent foreign nodes from being physically present in the network, especially when they remain passive. Besides, legitimate nodes that are unattended can be physically compromised.
- *Open channel*: WSNs rely on multi-hop wireless channels for communication. As wireless communication uses a broadcast channel, eavesdropping by foreign or compromised nodes cannot be prevented.
- *Distributed configuration*: WSNs inherit the properties of a wireless ad hoc network, where fixed infrastructure is not a necessary component. As a result, conventional access control models, such as role-based access control (RBAC) [13], that generally rely on a central Certificate Authority (CA) for authorization, are not applicable.
- *Constrained resources*: Cryptography and authentication mechanisms on which traditional access control models are based are common approaches for network security [14–16]. However, these cryptographic methods require high memory usage and power consumption because of their complex algorithms and processes [17], which is not practical for a resource-constrained WSN. Furthermore, cryptographic mechanisms may fail to prevent compromised nodes from launching attacks from inside.
- *Multi-vendor support*: WSNs may consist of sensor nodes from two or more manufacturers. Due to the different specifications and designs, it is difficult to ensure consistency in security implementation among all sensor nodes. This gives rise to the need for multi-domain access control, which is also considered in our proposed design.

In this paper, we propose a distributed and fine-grained access control model (TC-BAC) that aims to address the challenges mentioned above. We first introduce a trust evaluation mechanism into our access model where only trustworthy nodes are allowed to join the WSN. This can offer an effective solution to meet the security needs of an access control system with the absence of CA. Secondly, a risk function is proposed to assess the good behavior of a node and evaluate the risk factor of that node's access. These evaluations of trustworthiness and good behavior must be performed under a distributed environment by resource-constrained nodes. In our design, we adopt an access control mechanism that makes local authorization decisions based on the trust and centrality degree of other nodes. Finally, our design takes multi-domain access control into account and solves this problem by utilizing a mapping mechanism and group access policies.

The rest of this paper is organized as follows. Section 2 provides a brief overview of related work. Section 3 proposes the system model. Section 4 describes our proposal of distributed trustworthiness evaluation of nodes, followed by the proposal of distributed risk analysis based on centrality degree in Section 5. We provide detailed operation of our proposed solution, TC-BAC, in Section 6, with simulation results and performance evaluation given in Section 7. Finally, important conclusions and potential future works are given in Section 8.

2. Related work

Access control models have received considerable attention in research in recent years [18–20]. In these models, improving the performance of access control process is an important research issue. However, security assurance of the network remains as a main concern in access control schemes. It is worth emphasizing that the study of access control has a significant difference from admission control [21]. The design of access control schemes should follow the principles of security, while the admission control schemes mainly focus on QoS guarantees and resource reservation in the network [22].

Generally, there are three types of fundamental access control methods; namely, Mandatory Access Control (MAC) [23], Discretionary Access control (DAC) [24] and Role-based Access Control (RBAC). A MAC method controls access on the basis of security labels attached to the users and objects. Classified and static users must be predefined. This approach is particularly suitable for multilevel secure military environments. A DAC method controls access to an object on the basis of an individual user's permissions and/or denials, which gives flexibility to the access control with dynamic user information. This approach is practical for the security needs of industry and other non-military systems [13].

An RBAC method can be seen as an independent component of access control, coexisting with MAC and DAC when appropriate. RBAC was first introduced in [25] and the related standard was proposed after a series of modifications [26]. The main characteristic of RBAC is that all the mechanisms are based on a level of relations between users and roles. The users apply for various roles according to their tasks and then the administrators assign corresponding privileges to the users with specific roles. RBAC is fine-grained and adaptive for many dynamic systems including WSNs. However, conventional RBAC does not discuss the details of the security mechanisms. In many application scenarios, sensitive information should be accessible only to authorized users. If the attackers gain rights from different roles, they can easily cause great damage to inherent systems.

Please cite this article in press as: J. Duan et al., TC-BAC: A trust and centrality degree based access control model in wireless sensor networks, Ad Hoc Netw. (2013), http://dx.doi.org/10.1016/j.adhoc.2013.05.005

Driven by the demand for security considerations, some extended solutions to access control have been proposed for WSNs [27–29]. Role Based Access in Sensor Networks (RBASH) [30] is an access control model that provides multilevel security in sensor networks. In this model, the sensor nodes are divided into different levels according to an application's needs. The multilevel security is based on assigning keys to different nodes at different levels. To achieve this, the base station communicates with the cluster head to compute the cluster head key, and, by using a Hasse diagram, the cluster head works out other individual keys. However, these designs may cause high overhead, especially for the cluster head. Besides, when the cluster head is compromised, the protection of the sensor network will be disabled.

In 2009, Yu et al. proposed FDAC as a fine-grained distributed access control scheme [17]. FDAC exploits a novel cryptographic algorithm called attribute-based encryption (ABE). In FDAC, each sensor node is associated with a set of attributes and a public key. Each user is assigned an access structure, which is implemented via an access tree and embedded in the user's secret key. Having predefined keying materials for each of the attributes, the sensor data should be encrypted under the keys corresponding to their attributes and only those whose access structures accept the data attributes are able to decrypt. However, the complexity of computation and communication overload is directly proportional to the number of attributes in this strategy. Consequently, a high demand on computing and communication is required to implement the solution, which limits its attractiveness for WSN application. In addition, as the solution mainly utilizes cryptographic primitives, it is unable to prevent an internal attack from a compromised legitimate sensor node.

The realization of homomorphic encryption offers a new technique to perform cryptography in WSNs [16,31]. With homomorphic encryption, computations on plaintexts can be performed directly on the corresponding ciphertexts, and the decrypted ciphertexts after the computation process will always match that of the plaintexts undergoing the same computation process [32]. Its ability to meet the stringent end-to-end security requirements of typical security-critical applications makes it appropriate for distributed systems such as WSNs. Although this technique can significantly reduce the overhead of the multi-hop communication under the premise of security assurance, it requires a relatively complicated calculation and key generation process. Besides, similar to cryptographic primitives, the homomorphic encryption cannot defend internal attacks from a compromised sensor node.

Trust management is another vital type of approach that can fulfill the security requirements of access control systems [33,34]. Trust is often defined as a set of relations among entities. It has been demonstrated that by combining trust with specific protocols, the trust management in WSNs could be a useful complement to a public key infrastructure (PKI) [35–37]. Yang et al. incorporated the concept of trust into an RBAC model and presented an infrastructure-centric framework [38]. This model supports dynamic authorization according to trust level that is evaluated through infrastructure. The entities with good behavior will be rewarded and the others will be punished. Although these designs offer reliable solution to prevent internal attacks, the need for a central infrastructure limits its application to WSNs.

To enable the use of trust management in WSNs, there is a need for decentralizing it. Boukerche et al. proposed an agent-based trust scheme for WSNs [39]. It is assumed that a WSN is based on a mobile agent system that maintains the trust and reputation locally. The mobile agent is a trusted authority responsible for authenticating sensor nodes in the network. However, solely trusting mobile agents is idealistic and poses risks. In addition, passive attacks may occur outside of the direct coverage of mobile agents, and these attacks may remain undetected.

Risk assessment may offer a mechanism to evaluate trustworthiness, thus giving the ability to each node to detect misbehavior and exchange such information. In other words, risks are considered when when involving the trust into a specific application [40–42]. One common approach is the analysis of past behavior to assess the risk of trusting a particular node or granting it access control.

In [42], instead of incorporating trust, the authors proposed using the OASIS language to predicate the risk threshold. The semantics can encode the policies to provide the secure functionality. Karyotis et al. then designed topology control algorithms for the development of effective attack strategies by utilizing the risk factor [40]. This work described three topology control algorithms to analyze the infection of the nodes in the network. The attack model was constructed for the effective design of network countermeasures. However, the definitions of risk in previous work were ambiguous and most of them did not combine the risk degree with the trust evaluation process. To our best knowledge, no comprehensive study of the access control risk based on trust for WSNs has been made. In this paper, we propose a risk function to evaluate the security of the access control model. The main features of above solutions to access control are summarized in Table 1.

3. System model

3.1. Network model

In this paper, we consider a WSN consisting of a few sink nodes and a number of ordinary sensor nodes that are randomly distributed in a designated area. Each sensor node is identifiable by its unique ID. Both the sink nodes and the ordinary nodes are resource-constrained. Each ordinary sensor node is in charge of sensing its local conditions, initiating packets as a source, and forwarding packets as a router. There is no central CA for authorization deployed in the WSN. Sensor nodes that attempt to have access to the network must acquire certain access rights from other nodes that have already gained the corresponding privileges.

3.2. Security model

Due to the open and remote deployment environment, WSNs are generally vulnerable to physical attacks. In this

Please cite this article in press as: J. Duan et al., TC-BAC: A trust and centrality degree based access control model in wireless sensor networks, Ad Hoc Netw. (2013), http://dx.doi.org/10.1016/j.adhoc.2013.05.005

Table 1
The main features of solutions to access control.

Solutions	Methodology	Flexibility	Security	Complexity	System architecture	Drawbacks
MAC [23]	Based on security labels attached to the users and objects	Low	Low	Low	Centralized/ distributed	Lack of flexibility and scalability
DAC [24]	Based on an individual user's permissions and/or denials	Medium	Low	Low	Centralized/ distributed	Not fine-grained
RBAC [25]	Based on a level of relations between users and roles	High	Low	Low	Centralized/ distributed	Docs not discuss the details of the security mechanisms
RBASH [30]	Based on assigning keys to different nodes at different levels	High	High	High	Centralized	High overhead Exist the bottleneck of cluster head
FDAC [17]	Based on the asymmetric encryption and an access structure	High	High	High	Centralized	Requires a high demand on computing. Unable to prevent internal attacks
Homomorphic encryption [16]	Based on the fully homomorphic encryption technique	High	High	Medium	Centralized/ distributed	Needs a complicated calculation and key generation process. Unable to prevent internal attacks
TRBAC [38]	Based on the trust evaluation through infrastructure	High	Medium	Low	Centralized	Not adaptive for the distributed environment in WSNs. Pose a certain degree of risks
ATRM [39]	Based on a mobile agent system that maintains the trust and reputation locally	Medium	Medium	Low	Distributed	Do not takes multi-domain access control into consideration

paper, we assume that all of the ordinary sensor nodes are compromisable. Compared with them, the sink node has a higher ability to resist common attacks because of its more sophisticated hardware. They can thus be recognized as a highly trusted party in most cases. Even if a sink node is compromised, other sink nodes in the network could seize its malicious behavior. We also assume that ordinary nodes have a higher probability to be compromised if one or more of their neighbors are malicious.

Our access control model aims to protect information and operation of WSNs from being compromised by malicious nodes. These malicious nodes may be foreign nodes being covertly introduced into a network or legitimate nodes being physically compromised. These malicious nodes will attempt to join the networks as legitimate nodes and then launch attacks either passively or actively. In passive attacks, malicious nodes may gather sensitive information or behave selfishly in collaborative operations, such as routing, to passively affect the proper operation of WSNs. In active attacks, malicious nodes may actively request sensitive information, influence the behavior of surrounding nodes [43], or affect the normal operation of WSNs using attacks such as Denial of Service (DoS).

In our access control model, we first utilize trust to ensure that only legitimate nodes are permitted to join WSNs and then centrality degree to continually assess risk of access. Briefly, each node stores a local trust matrix based on the records of other nodes' behavior and a centrality degree attribute that represents its importance in the network. We assume that the network owner can configure the privileges of each node through the sink node.

4. Trust degree evaluation

4.1. Architecture of trust management

In this paper, we consider trust in sensor networks as the degree of beliefs about the behavior of other ones. According to the characteristics of WSNs, the architecture of trust management for access control is depicted in Fig. 1.

Data streams are the source of the evidence of trust in trust management schemes. By adopting some related detection mechanisms, such as watchdog [44], sensor nodes can seize malicious or selfish behavior (e.g. packet flooding, packet dropping, or wormhole attacks). The trust of an arbitrary node in the network includes two parts: direct trust and indirect trust. Direct trust is based on direct observations of each node that participates in data communication, while indirect trust stands for the trust relations between distributed nodes without direct interactions, which can be seen as recommendation trust or reputation.

As an error probability of detection may exist in the detection mechanisms, a malicious node that provides false trust value may be incorrectly included in the trusted set of nodes. To solve this problem, we adopt an inconsistency check scheme [45] in trust collection process (collecting data of direct trust and indirect trust) to detect malicious nodes and filter out false trust values. More specifically, a set of rules is defined in the nodes' inconsistency checking module to check the inconsistence of indirect trust values. If a "bad" node provides false trust value, it can be quickly detected as its false recommendation may have a significant difference (higher or lower) from true ones provided by other nodes in the trusted set.

Since trust is about a node's attitude towards others' behavior, our access control model utilizes it to construct specific policies. To further support multiple vendors, we include the concept of domains in our design. In the following subsections, we first describe trust evaluation in a single-domain, then extend our design to the case of multiple-domains.

4.2. Trust evaluation in a single-domain

The trust evaluation on which most of the prior work mainly focuses is the key problem of trust management

Please cite this article in press as: J. Duan et al., TC-BAC: A trust and centrality degree based access control model in wireless sensor networks, Ad Hoc Netw. (2013), http://dx.doi.org/10.1016/j.adhoc.2013.05.005

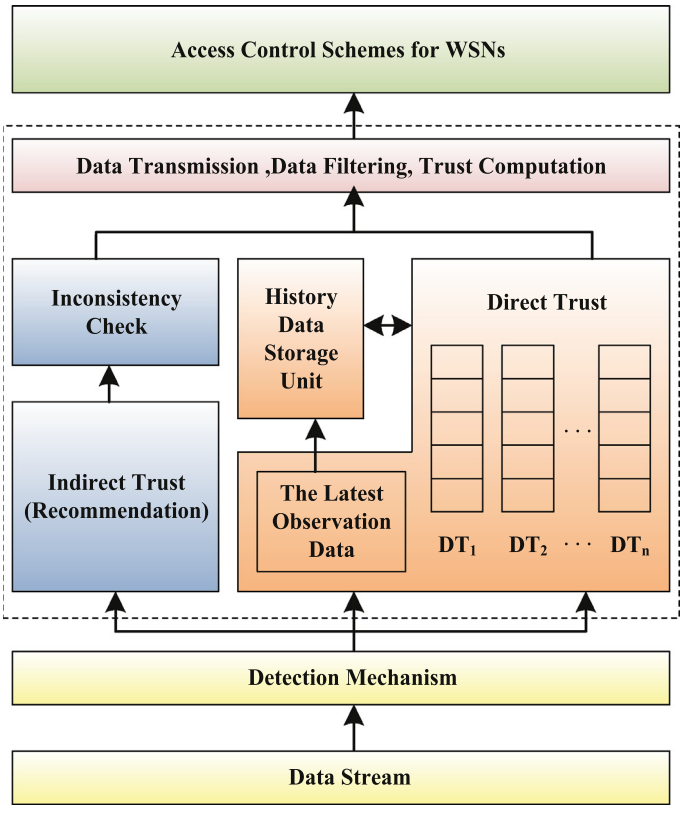


Fig. 1. The architecture of trust management.

scheme. In [35,36], the authors proposed the requirements and principles which should be followed when designing trust evaluation algorithms. They also discussed the basic algebraic properties and the optimizing characteristics of trust metrics by utilizing mathematical tools, such as the theory of semirings. We follow these basic principles in the following formulation and evaluation.

First, we will discuss the WSN that is deployed in a single domain, which is depicted in Fig. 2a. All the sensor nodes share similar specifications and operate under a single administrator. Thus, every node uses the same method to measure trust values. To evaluate the nodes' trust in the single-domain, we propose a trust computational method. As is shown in Fig. 1, the trust is composed of direct trust and indirect trust. The former can also be divided into two units: the latest observation data unit and the history trust data unit that stores trust records between sensor nodes in a specified structure, while the latter is obtained from recommendations of other nodes. The trust evaluation process can be represented as follows:

$$T(i_X,j_X)^l = \alpha_1 \times DT(i_X,j_X)^l + \beta_1 \times \frac{\sum_{(k\in N_j,k\neq i)} IT(k_X,j_X)^l}{|N_j|-1} \quad (1)$$

with $\alpha_1 + \beta_1 = 1$, $\alpha_1 > 0$, $\beta_1 > 0$. As in Eq. (1), $Ti_X, j_X)$ represents the trust value of node j for node i in a single-domain **X**. Node i measures the trust of node j based on both direct trust, $DT(i_X, j_X)$, and indirect trust $IT(k_X, j_X)$ in domain **X**. The quantity l represents the sequence number of the latest evaluation records. In the term of indirect trust, N_j is a set consisting of neighbors of node j. The reason we choose the indirect trust value provided by the neighbor nodes is that most malicious behavior can be detected by the neighbors and this mechanism can obviously reduce the overhead of the network.

The quantities α_1 and β_1 are weight factors which are associated with the access control policies. Setting $\alpha_1 > \beta_1$ indicates that the node in the network is more convinced about its own judgement than other nodes judgements. Setting $\alpha_1 < \beta_1$ indicates that it prefers to rely on recommendations by others in trust evaluation. The trust value is bounded by $0 \leqslant T \leqslant 1$ where a higher value indicates higher trustworthiness.

The evaluation of direct trust is given by:

$$DT(i_X,j_X)^l = \gamma \times DT(i_X,j_X)^{l-1} + E(i_X,j_X)^l \quad \gamma > 0 \quad (2)$$

where $DT(i_X, j_X)^{l-1}$ represents the direct trust value based on the past behavior of the node. The $E(i_X, j_X)^l$ represents the current behavior of a device. The weighed factor γ is an exponential decay time factor, which is computed by:

$$\gamma = e^{-\rho\times(t_c - t_{c-1})} \quad t_c > t_{c-1} \geqslant 0, \quad \rho \geqslant 0 \quad (3)$$

where t_c stands for the current time and the t_{c-1} represents the time when the last interaction occurred. According to Eq. (3), the trust value decreases with the passage of time. The weight factor should depend on the context. When $\gamma \ll 1$, it means that the results of recent interactions are

Please cite this article in press as: J. Duan et al., TC-BAC: A trust and centrality degree based access control model in wireless sensor networks, Ad Hoc Netw. (2013), http://dx.doi.org/10.1016/j.adhoc.2013.05.005

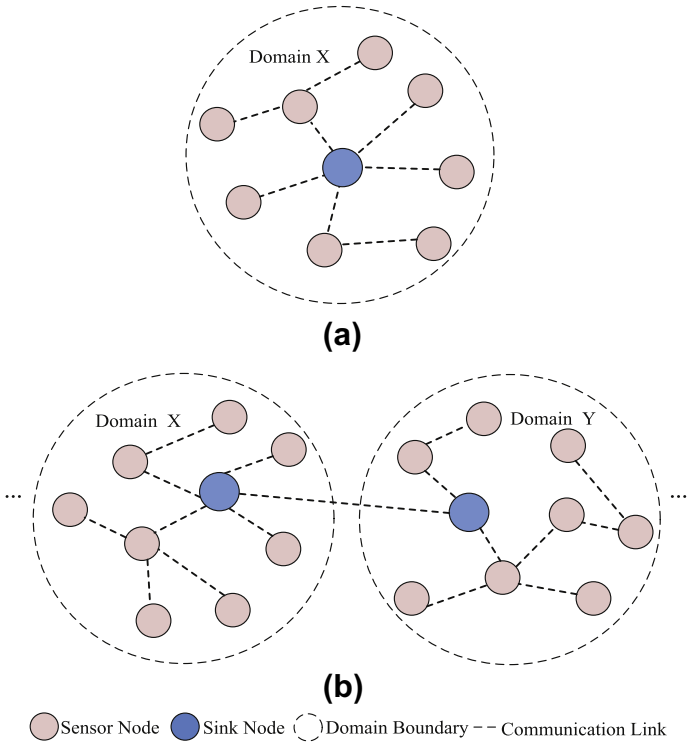


Fig. 2. (a) WSNs in single-domain and (b) WSNs in multi-domain.

much more important than those of older ones. However, in this case, malicious nodes may easily eliminate their bad reputation through short-term actions when they intend to communicate with other nodes.

The function $E(i_X, j_X)^l$ is given by:

$$E(i_X,j_X)^l = \begin{cases} P(a), & for\ 0 < P(a) < 1 \quad (4) \\ N(a), & for\ -1 < N(a) < 0 \quad (5) \end{cases}$$

where $P(a)$ and $N(a)$ represent the positive and negative assessment for the node's action a, respectively. These two parameters should follow the common practice that a good reputation is more difficult to gain than a bad one.

Finally, the indirect trust evaluation process is computed by:

$$\sum_{k\epsilon N_j, k\neq i} IT(k_X,j_X)^l = \sum_{k\epsilon N_j, k\neq i} DT(i_X,k_X)^l \times DT(k_X,j_X)^l. \quad (6)$$

In the above, the indirect trust value of node j for node i is computed by recommendations from the neighbors of node j. In this model, we employ the trust chain to evaluate the indirect trust of the node.

4.3. Trust evaluation in multi-domain

As mentioned in Section 1, a WSN may consist of sensor nodes from different vendors or deployed by different service providers. To support this scenario, a WSN can be logically divided into several administrative groups and each group may possess its own methods to evaluate trust with some sharing of trust information across groups, as illustrated in Fig. 2b. Therefore the trust evaluation mechanism in multi-domain situations requires additional attention to features of the inter-domain sharing of trust information.

The trust of one domain for another is determined by the trust relationship between the two domains [46]. To address trust evaluation problems in multi-domain situations, we design a mapping mechanism. Let X, Y and Z be the sets collecting the identities of all nodes within domains **X**, **Y** and **Z** respectively, and let V be the set containing all domain sets in a WSN. The trust evaluation process in multi-domain situations can be described by the following expressions:

$$T(i_X,j_Y)^l = M(X,Y)^l \times T(Y,j_Y)^l \quad (7)$$

where $T(i_X, j_Y)$ represents the trust value of node j in a domain **Y** for node i in an another domain **X**. The function $M(X, Y)$ represents the mapping mechanism between these two domains. The value $T(Y, j_Y)$ is the average trust value of node j in its own domain **Y**. The mapping mechanism can be further described as below:

$$M(X,Y)^l = \alpha_2 \times \mathrm{SP}(X,Y)^l + \beta_2 \times \frac{\sum_{(Z\in V, Z\neq X, Z\neq Y)} IT(Z,Y)^l}{|V|-2} \quad (8)$$

with $\alpha_2 + \beta_2 = 1$, $\alpha_2 > 0$, $\beta_2 > 0$. The function $\mathrm{SP}(X, Y)$ refers to a security policy parameter from domain **Y** to domain **X**. $IT(Z, Y)$ is the recommendation from other domains.

$$\mathrm{SP}(X,Y)^l = \phi \times V(X,Y)^l + \varphi \times \frac{\sum_{k_Y\epsilon Y} DT(X,k_Y)^l}{|Y|}, \quad (9)$$

Please cite this article in press as: J. Duan et al., TC-BAC: A trust and centrality degree based access control model in wireless sensor networks, Ad Hoc Netw. (2013), http://dx.doi.org/10.1016/j.adhoc.2013.05.005

with $\phi + \varphi = 1$, $\phi > 0$, $\varphi > 0$. $V(X, Y)$ is configured by vendors or service providers in advance; thereby, it can be seen as the trust between the service providers. $DT(X, k_Y)$ stands for the direct trust value of node k_Y of domain **X**, which can be acquired from the interactions between domain **X** and domain **Y**. The indirect trust value of domain **Y** for domain **X** is computed by recommendations from other domains in the network:

$$\sum_{(Z\in V, Z\neq X, Z\neq Y)} IT(Z,Y)^l = \sum_{(Z\neq X, Z\neq Y)} \mathrm{SP}(X,Z)^l \times \mathrm{SP}(Z,Y)^l. \quad (10)$$

The trust value of the target node j in its own domain **Y** is given by:

$$T(Y, i_Y)^l = \frac{\sum_{(k\in N_j, N_j\subset Y)}^{|N_j|} T(k_Y, j_Y)^l}{|N_j|}, \quad (11)$$

where $T(k_Y, j_Y)$ represents the trust value of node j for its neighbors in the same domain **Y**. The trust evaluation methods in multi-domain situations are available for practical applications. Based on these methods, we introduce a group access mechanism in Section 6.

5. Centrality degree and risk analysis

5.1. Centrality degree evaluation

The concept of centrality degree comes from social networks. It is used to analyze the relations among the entities in the network. For example, a higher centrality degree for a given person may imply that he attracts more attention than usual from other people. Instead of using the centrality degree to measure the relations between nodes, we utilize it in our access control model to evaluate the risk factor when adopting the distributed systems. We can then make reasonable security policies to reduce the risk ratio to meet a certain protection level. In this section, we first propose a method to measure the node's centrality degree.

As is shown in Fig. 3, the node's centrality degree in the network is composed of the rank of the access ring and the number of the node's neighbors. The access ring can be defined as the set of sensor nodes which have the same routing distance from the sink node. For example, the access ring of node *A* is ranked at layer two, and node *A* has four neighbors which are nodes *B*, *C*, *D* and *E*. Based on this information, we propose the following method to evaluate the centrality degree of node i, $\mathrm{CD}(i)$:

$$\mathrm{CD}(i) = \omega \times \frac{\mathrm{Max}(R(N))}{R(i)} + \lambda \times |N_j| \quad (12)$$

where $\omega + \lambda = 1$, $\omega > 0$, $\lambda > 0$. The function $R(i)$ represents the access ring of the node i. The quantity N is the set of nodes in the network, $\mathrm{Max}(R(N))$ represents the largest value of access ring in the network, and $|N_j|$ is the number of the neighbors of node j.

5.2. Risk function

Introducing trust levels into access control schemes will definitely benefit distributed systems. However, the lack of a CA in a distributed system poses a risk. Thus, we use risk assessment to evaluate the risk of granting an access control. In our model, the risk function mainly depends on the node's centrality degree and average trust degree in the network. As the malicious node may compromise its neighbors, we also take the neighbors' risk factors into consideration. The node's centrality degree in the network is composed of the rank of the access ring and the number of neighbors for each of the nodes. There are two main reasons for choosing this mechanism for risk assessment. First, it is intuitive that with a shorter distance to the sink node, a malicious node can be more successful in intercepting communications and launching attacks. Secondly, a malicious node with more neighbors generally has higher influence in the network. A malicious node may use this influence to quickly gain trust before launching an attack.

As explained above, we propose a risk function in WSNs, which is given by:

$$R_F(j) = \mu \times \left(\mathrm{CD}(j) + \frac{\pi \times |N_j|}{\sum_{k\in N_j} T(k,j)^l} \right) + P_c \times \sum_{k\in N_j} R_F(k) + v \quad (13)$$

where $R_F(j)$ is the risk value of node j. We note that faor sink node s, $R_F(s) = 0$ which means that trusting the sink node is risk free. The term $\frac{\sum_{k\in N_j} T(k,j)^l}{|N_j|}$ gives the average trust degree of node j in the network. The quantity P_c is the probability that a node is compromised, and N_j is a set collecting all neighbors of node j. Finally, the values of the parameters μ, v and π are to be set empirically and can be adjusted dynamically.

Based on the risk function, the administrator can set up the access control policies in the sensor nodes. When a newly arriving node tries to join the network, the access model can evaluate its risk factor by using the risk function and then determine whether to permit an access operation.

6. TC-BAC schemes

6.1. The basic framework of TC-BAC model

The classical access control model RBAC has attracted a lot of interest in many areas. The main property of this model is the assignment of predefined roles to users. Users with different roles may have different privileges, which can provide the network with fine-grained control. However, it is unsuitable for distributed systems, especially WSNs. In this paper, we propose a distributed and fine-grained access control model based on the RBAC. The basic framework of our model is presented in Fig. 4. Our main idea is the introduction of the trust and centrality degree attributes into the RBAC model to make it practical for WSNs. The access control framework consists of the following components:

- Administrators (A) – The entities that include constraints to adjust the set of permissions, trust levels, security policies and the user assignments. In our model, the administrator is the sink node or someone who has rights to control the sink node in the network.

Please cite this article in press as: J. Duan et al., TC-BAC: A trust and centrality degree based access control model in wireless sensor networks, Ad Hoc Netw. (2013), http://dx.doi.org/10.1016/j.adhoc.2013.05.005

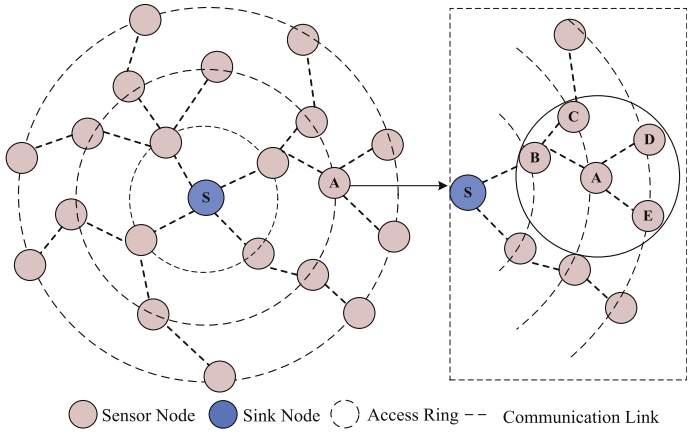


Fig. 3. The metric of centrality degree in sensor networks.

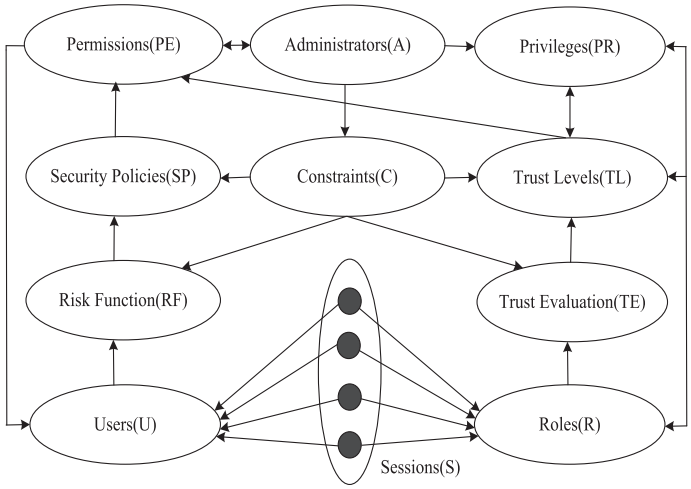


Fig. 4. The basic framework of TC-BAC model.

- Permissions (PE) – A description of authorized interactions that determine whether a new access request can be granted. The results of the permissions can be fed back to the administrators, enabling dynamic adjustment of constraints for the network.
- Constraints (C) – The clauses that can modify the permissions, trust levels, security policies and the user assignment, which is instituted by the Administrators.
- Security Policies (SP) – A set of rules used to limit the security risk. It is a part of inputs to the permissions.
- Trust Levels (TL) – The trust values that measure the trustworthiness of a node. The trust level is also a part of the input to the calculation and granting of permissions. It is associated with specific roles.
- Privileges (PR) – The rights approved in the network, which are related to the users' roles.
- Risk Function (RF) – A function that evaluates the risk factor of a newly arrived user.
- Trust Evaluation (TE) – The computational process that evaluates the user's trust.
- Users (U) – The entities who want to join the network. In this model, the users are simply sensor nodes.
- Session (S) – A mapping process between the users and roles.
- Roles (R) – The job functions that describe the authority and responsibility of the users. A user who joins the network must be assigned to a specific role.

Based on the above attributes in the access control model, we use the following simplified expressions to describe operations and outcomes. These expressions are used in our algorithm description.

- $U \otimes TE \rightarrow UTE$: A user is evaluated by our proposed trust computational process, and the outcome is given in *UTE*.
- $UTE \otimes TL \rightarrow PE_T$: A computed trust value is measured against a trust level. The outcome is given in PE_T which carries a boolean value. A "true" indicates the computed value crosses the trust level and permission can be granted, and "false" indicates otherwise.

Please cite this article in press as: J. Duan et al., TC-BAC: A trust and centrality degree based access control model in wireless sensor networks, Ad Hoc Netw. (2013), http://dx.doi.org/10.1016/j.adhoc.2013.05.005

- $U \otimes RF \rightarrow URF$: A user is evaluated by the risk function, and the outcome is given in URF.
- $URF \otimes SP \rightarrow PE_R$: A risk value is measured against the security policies in the network. The outcome is given in a boolean value PE_R. A "true" indicates the riskiness is believed to be under control, and "false" indicates otherwise.
- $PE_T \cap PE_R = = PE$: Both the trust degree and the risk degree satisfy the demand for security.
- $U \otimes R \rightarrow PR$: If the user has access to the network, it could obtain the corresponding privileges according to its applying role.

Algorithm 1. The access control algorithm of TC-BAC

```
1: Process Initialization
2: if New Node Ready then
3:     Send Access Request U = ⟨u_id, r, t, key_join⟩
4: end if
5: if Access Request Received then
6:     if Have Access Privilege then
7:         Send Trust Request
8:     else
9:         return NULL
10:    end if
11: end if
12: if Trust Request Received then
13:    Send Trust Reply
14: end if
15: if Trust Value Updated then
16:    U ⊗ TE → UTE
17:    if UTE ⊗ TL → PE_T then
18:        U ⊗ RF → URF
19:        if URF ⊗ SP → PE_R then
20:            if PE_T ∩ PE_R = = PE then
21:                U ⊗ R → PR
22:                return PE
23:            end if
24:        else
25:            return P̄E
26:        end if
27:    else
28:        return P̄E
29:    end if
30: end if
31: END Process
```

6.2. TC-BAC in a single-domain situation

The trust and risk factor are crucial parameters for determining whether a node is acceptable. The higher the trust value a node has, the easier it can join the network. Similarly, if a node has a lower risk, it is more likely to be granted access rights. In our model, a newly arriving node is not permitted to join the network unless both of these attributes satisfy the requirements.

Not all nodes in the network have the privilege to allow the newly arrived node to join the network. Depending on the context, this privilege is set by the administrators. In addition, the TC-BAC is a flexible access control model. It is not only designed for the sensor network without central CA for authorization, but is also an optional scheme for the one that has the complete authentication system. If a newly arriving sensor node has the key-join (a key used to join the network), it will obtain a high trust degree immediately.

In a single domain, each node has the same trust evaluation method and security policies. The process that a newly arriving node follows to join the network in a single domain is shown in Fig. 5. More specifically, the TC-BAC scheme in the single-domain case works as follows (see also Algorithm 1 outlining the pseudocode of access control process):

Step 1. The newly arriving node N sends the request to the destination node D. In this model, the access request is a 4-ary tuple, and is denoted as $U = \langle u_{id}, r, t, key_{join} \rangle$, where u_{id} is the source node's ID, r is the role that the node request to activate, and t is the timestamp. Furthermore, the request node may include the key-join if it has one.

Step 2. When the destination node receives the request, it should check whether it has the rights to allow the new node to join the network. If it has, it will compute the direct trust value of the new node and send a trust request to the neighbors of the new node to obtain their recommendations (broadcast the request with finite TTL). The neighbor list can be updated by the existing neighbor discovery process, by, for example, the interactions of periodic "hello" packets.

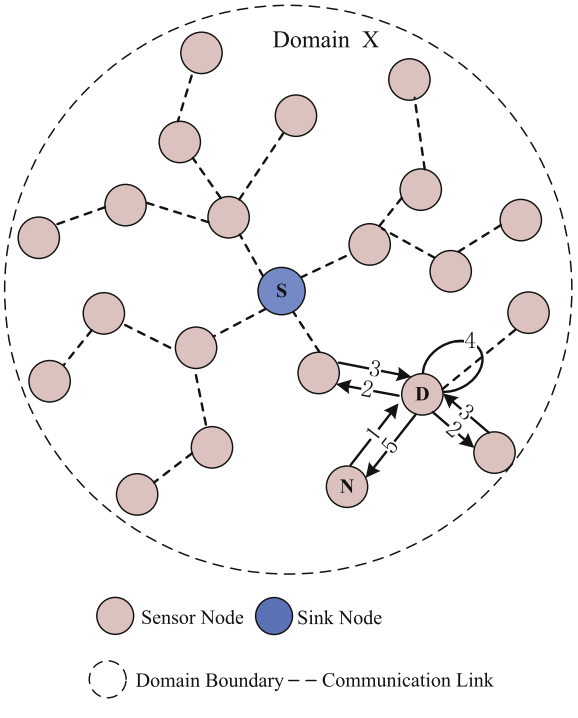


Fig. 5. The access control model in a single-domain.

Step 3. The nodes that receive the trust request will check whether they are the requested objects. If they are, they will send a trust reply. Otherwise, they simply keep silent.

Step 4. After obtaining the recommendations, the node D generates a local trust matrix to compute the trust value of the new node by Eq. (1). The local trust matrix is given by:

$$\begin{bmatrix} DT(i_X,j_X)^{l-m+1} & IT\left(k_X^1,j_X\right)^{l-m+1} & \cdots & IT\left(k_X^{|N_j|-1},j_X\right)^{l-m+1} \\ DT(i_X,j_X)^{l-m+2} & IT\left(k_X^1,j_X\right)^{l-m+2} & \cdots & IT\left(k_X^{|N_j|-1},j_X\right)^{l-m+2} \\ \vdots & \vdots & & \\ DT(i_X,j_X)^{l} & IT\left(k_X^1,j_X\right)^{l} & \cdots & IT\left(k_X^{|N_j|-1},j_X\right)^{l} \end{bmatrix}$$

where $DT(i_X, j_X)^l$ and $IT\left(k_X^{n-1},j_X\right)^l$ represents the latest direct trust value from node j to node i and indirect trust value from node j to node k^{n-1}, respectively. Node j is the one that requests to join the network and node i is the handling the request. The quantity m is the number of history records and n is the number of node j's neighbors. In addition, the new node that has the key-join must be considered as owning a high trust level when it has no history records in the network. However, the key-join should be void when the node gains a bad reputation in the network. This prevents a compromised node from launching an internal attack. When the new node passes the trust evaluation process, risk assessment takes over to measure the risk of access.

Step 5. The destination node D should decide whether to grant permission to the newly arriving node N. As the destination node may be corrupted, we think that it is unsafe if the decision to give or not give permission to a new arrival node to join the network is made by only one node. In accordance with the above process, the newly arriving node will have access to the network and obtain the corresponding privileges when it receives more than two certificates from different destination nodes.

As the destination node needs to contact with neighbors to obtain their recommendations, the time complexity of TC-BAC in a single-domain is $O(|N|)$, where $|N|$ is the number of neighbors which provide the recommendations. All the users in the network have their unique IDs. This is a key property in trust-based schemes; otherwise, an intruder could just claim different IDs once its trust value declined. Some work has already been performed in this area [20,27], which is not in the scope of this paper.

The initial trust of a newly arriving node is based on the local security policies. Generally, a new node without adverse records should be accepted if the risk factor is believed to be under control. If the newly arriving nodes are initially rejected, they can send requests to other access points or lower their roles requested in their application to obtain the opportunity to earn trust.

When a node joins the network, its behavior will be evaluated by the neighbors. Each time a transaction takes place, the degree of trust and risk will be updated. If the trust level of a node falls below a threshold, the node will be evicted from the network. In other words, the nodes in the network will record the malicious nodes in their blacklists and all the messages from the malicious nodes in the blacklist will be dropped. The threshold should be set dynamically, which is associated with the trust value of the local network.

In order to deal with the false trust value caused by error detection and collusion attacks, we introduce a error probability of detection in our model and analyze its effect to the trust evaluation process, which is further discussed in Section 7.

6.3. TC-BAC in multi-domain

The access control model in multi-domain is important because WSNs may be formed by several autonomous groups wishing to share resources. However, each domain is likely to own the individual trust evaluation methods and security policies. So a mapping mechanism is designed for the situation that a node in one domain that wishes to gain an access to a network in a different domain, as introduced in Section 4. In this case, the sink node is responsible for negotiating and maintaining the information with other domains.

The process of a new node to join the network in a multi-domain situation is shown in Fig. 6.

Step 1. A newly arriving node, say node N, in domain **Y** sends a request to the destination node D in domain **X**. The request contains the necessary information of node N.

Step 2. When the destination node D receives the request, it should check whether it has the privilege to allow a node in another domain to join the network. If it has, it will send trust request to its sink node S_D. Node S_D that receives the trust request will forward the request to the sink node of another domain, say node S_N. Then node S_N evaluates the trust of node N in its local domain.

Step 3. After the trust evaluation process, the sink node S_N sends reply to the sink node S_D. Adding in the trust value from domain **Y** to domain **X**, the sink node S_D forwards the trust reply to node D.

Step 4. Then the destination node D generates the local trust matrix and computes the trust value of node N by Eq. (8). The local trust matrix is presented as follow:

$$\begin{bmatrix} SP(X,Y)^{l-m+1} & IT(Z^1,Y)^{l-m+1} & \cdots & IT(Z^{|V|-2},Y)^{l-m+1} & T(Y,j_Y)^{l-m+1} \\ SP(X,Y)^{l-m+2} & IT(Z^1,Y)^{l-m+2} & \cdots & IT(Z^{|V|-2},Y)^{l-m+2} & T(Y,j_Y)^{l-m+2} \\ \vdots & \vdots & & & \\ SP(X,Y)^{l} & IT(Z^1,Y)^{l} & \cdots & IT(Z^{|V|-2},Y)^{l} & T(Y,j_Y)^{l} \end{bmatrix}$$

When node N passes the trust evaluation process, the risk factor of the new node should also be analyzed in the same way.

Step 5. If the access request is accepted, the node D should issues a certificate to new node N. If the node N receives more than two certificates from different destination nodes, it will join the network and obtain the privileges corresponding to its role.

Please cite this article in press as: J. Duan et al., TC-BAC: A trust and centrality degree based access control model in wireless sensor networks, Ad Hoc Netw. (2013), http://dx.doi.org/10.1016/j.adhoc.2013.05.005

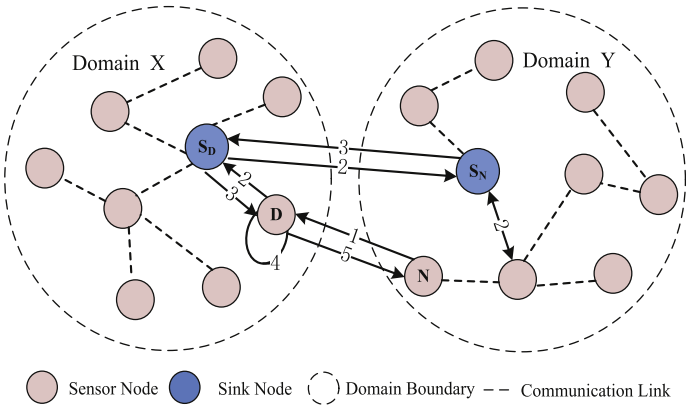


Fig. 6. The access control model in a multi-domain situation.

For multi-domain scenarios, the time complexity is $O(|N| \times |M|)$ where $|M|$ is the total number of domains in WSNs.

6.4. Group access

The group access defines a rapid access mechanism when a set of nodes that belongs to the same domain tries to join the existing network. This method can be considered as a specific form of the access control schemes in multi-domain. The group access mechanism can help improve the operational scalability, but it may also bring some additional risk. Whether to adopt the group access method depends on the security policies in the network. To reduce the risk factor, only sink nodes have the privilege to give permissions to a desired group. In this case, the time complexity of TC-BAC is $O(|M|)$.

The process of a new group to join the network is shown in Fig. 7.

Step 1. The sink node S_G in domain **Z** sends a request to the destination sink node S_D in domain **X**. The request contains the necessary information of the new group, which includes the nodes N_1 through N_8.
Step 2. When the sink node S_D receives the request, it should check whether it has the corresponding privilege. If the sink node S_D has the rights, the trust evaluation and risk analysis processes are launched. In this case, the trust level and risk factor are mainly based on the default parameters.
Step 3. If the access request is accepted, the sink node S_D should return the permission to the new group. Then the nodes in the new group can access the network accordingly.

7. Simulation results and performance evaluation

In this section, we focus on evaluating the access control model by performing relevant simulations. The simulations are done by NS-2 simulator [47]. We define two types of sensor nodes in the simulations: well behaved nodes and malicious nodes. The malicious nodes launch two types of attacks in the simulated scenarios. One is the selfish attack and the other is the DoS attack. The probability of each one is 50%. As described in [6,48], a selfish node only cares to transmit its own data packets and simply drops packets generated by others in multi-hop communications to preserve its resources. A DoS attacker in the simulated scenarios will attempt to disrupt legitimate communication of other nodes by flooding the network with unwanted traffic. All the default simulation parameters that we have chosen are summarized in Table 2.

Four simulation experiments are conducted to validate the effectiveness of our proposed scheme. Firstly, we analyze the trust evaluation process by considering the impact of the various vital weight factors. Secondly, we test the validity of the risk function. Thirdly, several metrics are measured to evaluate the performance of TC-BAC both in single-domain and multi-domain. Finally, the applicability of TC-BAC are discussed at the end of this section.

7.1. The analysis of trust evaluation

In our design, the weight factors are critical for the trust evaluation process. We select some important parameters which include the trust weight factors and the exponential decay time factor to analyze their effect on the trust evaluation.

As shown in Fig. 8, the trust value typically grows over time if no abnormal behavior occurs. By contrast, Fig. 9 illustrates the process with malicious behavior. In this case, the trust value decreases significantly due to the negative assessment for the malicious behavior.

The correctness of the trust evaluation is based on the accuracy of detection mechanisms. If all the behavior of nodes can be detected accurately, the indirect trust data are not necessary. To validate this, we introduce an error probability of detection in simulations. We first compare the results with an idealistic setup where error probability of detection is set to zero. The results for zero error probability of detection are called real trust values. The direct trust weight factor of the node is determined by how much a node should rely on its own judgment. As illustrated in Figs. 8 and 9, if the network can seize all the behavior of the node correctly, the higher the direct weight factor we

Please cite this article in press as: J. Duan et al., TC-BAC: A trust and centrality degree based access control model in wireless sensor networks, Ad Hoc Netw. (2013), http://dx.doi.org/10.1016/j.adhoc.2013.05.005

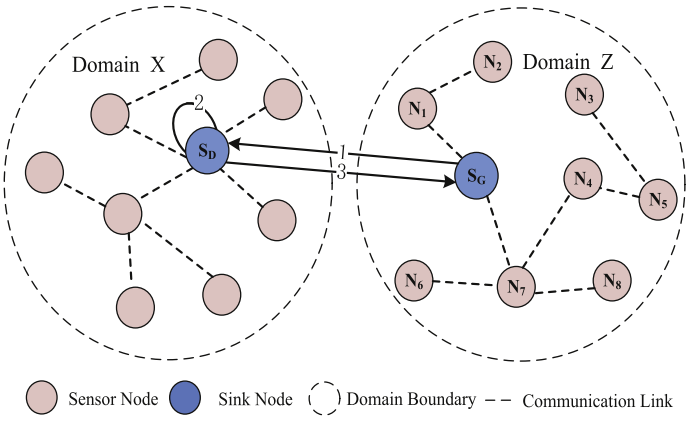


Fig. 7. The process of the group access.

Table 2
Simulation parameters.

Parameters	Values
Simulation time	500 s
Monitoring area	200×200 m^2
Number of nodes	100
Communication range	100 m
Packet interval	5 s
Length of data packet	100 bytes
Initial energy	1000 J
Transmit energy	0.090w
Receive/listen energy	0.075w
Idle energy	0.003w
Routing protocol	AODVjr [49]
MAC layer protocol	IEEE 802.11
Initial trust value	0.5
Distrust interval	[0, 0.2)
Error probability of detection	0.01
$P(a)$	0.01
$N(a)$	−0.15
ρ	0.001
α_1, α_2	0.5

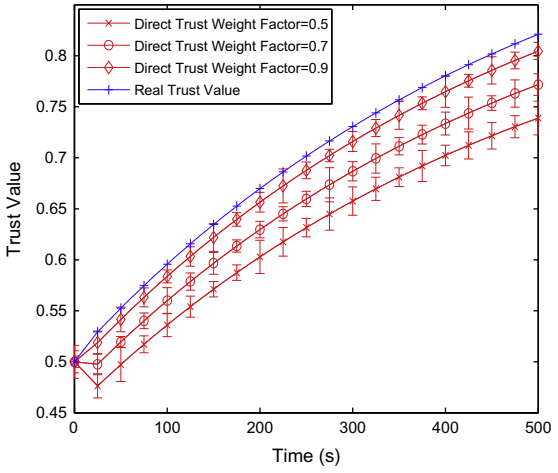


Fig. 8. The effect of DT for good behavior.

choose, the closer to the real value the calculated trust degree is. However, it is almost impossible to realize it in actual conditions as an error probability of detection may exist. In addition, a node cannot listen to the wireless communication channel all of the time because of energy constraints.

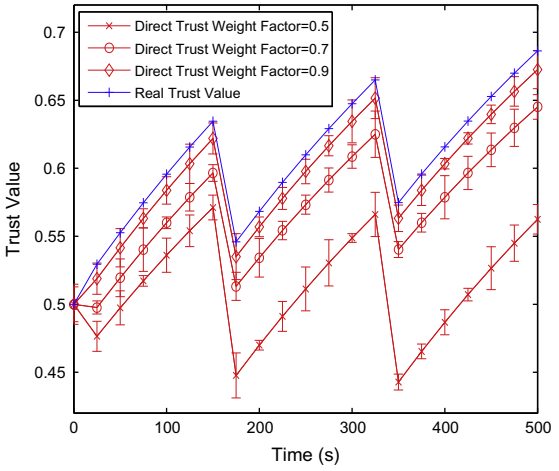


Fig. 9. The effect of DT for malicious behavior.

Then, we set the error probability of detection to 0.03. The error detecting events will cause the decrease of the trust value, which is illustrated in Figs. 10 and 11. From Fig. 10, we notice that if some error detecting events occur, the higher indirect trust weight factor can provide better resistance capability, which reduces the deviation from the real trust value. Because the indirect trust is normally composed of multiple recommendations provided by different nodes. It is obvious that its error probability is lower than the direct trust which is only based on a single node's detection. Similarly, more recommendations can also provide better resistance capability for the network, which is shown in Fig. 11.

Generally, the trust value should decrease with the passage of time. Fig. 12 presents the effect of the exponential decay time factor. The sensors in the network stop sending packets from 200 s to 300 s in the simulation. The higher decay time factor indicates that the historical trust data

Please cite this article in press as: J. Duan et al., TC-BAC: A trust and centrality degree based access control model in wireless sensor networks, Ad Hoc Netw. (2013), http://dx.doi.org/10.1016/j.adhoc.2013.05.005

will decrease quickly with time. Thus the nodes that wish to keep a high trust value must behave well in the latest transaction.

In addition, we notice that the trust value may decrease at the bootstrap time. Because the initial trust is set in advance and the recommendations provided by other nodes will not be trusted completely. Consequently, according to Eqs. (1) and (6), the calculated trust value is always below the initial trust after the first transaction.

7.2. The analysis of risk degree

In our design, the risk function is based mainly on the node's centrality degree, which is composed of the rank of the access ring and the number of the node's neighbors. We design three simulation tests to validate that a higher centrality degree indeed leads to a higher risk degree. In the first test, malicious nodes are excluded in order to study the effect of the load on the network performance. We intensify load by shortening the packet arrival interval. As illustrated in Fig. 13, the average packet delivery ratio drops as the network load intensifies. This is because when the load is high, network congestion appears and recommendation packet starts to drop. In the remaining tests, we set packet interval to 5 s in order to focus on condition without congestion.

Then, we select three groups of nodes from the different access rings, respectively. Each group includes three sensor nodes and has the same average number of neighbors. We assume these sensor nodes are malicious and then analyze their impact on the average packet delivery ratio of the network. As is shown in Fig. 14, the average packet delivery ratio is close to 100% (about 98.7%) when there are no attacks in the network. However, if there are some malicious nodes launching the attacks, the average packet delivery ratio will suffer a degradation. This phenomenon is more obvious when the malicious nodes stay in an access ring with lower rank (about 82.7% in layer 7, about 76.1% in layer 5, about 72.5% in layer 2). Similarly, in the second test, we choose two malicious nodes in the same access ring, and each node has the different number of neighbors. Fig. 15 illustrates the results of this test. The results show that a malicious node with more neighbors will indeed cause greater damage to the network.

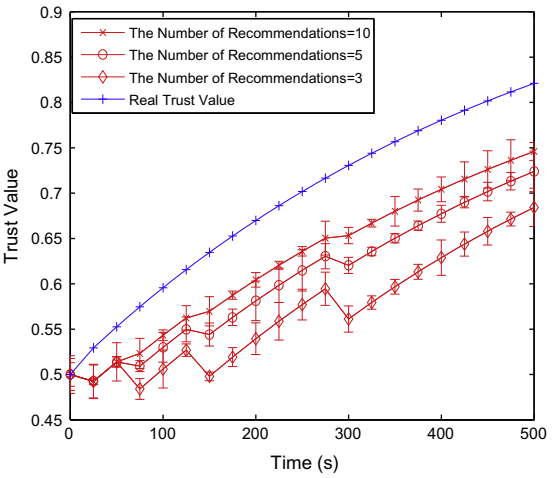


Fig. 11. The number of recommendations.

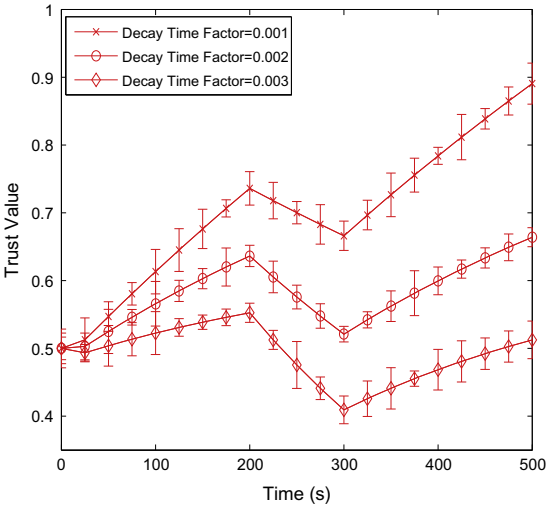


Fig. 12. The effect of decay time factor.

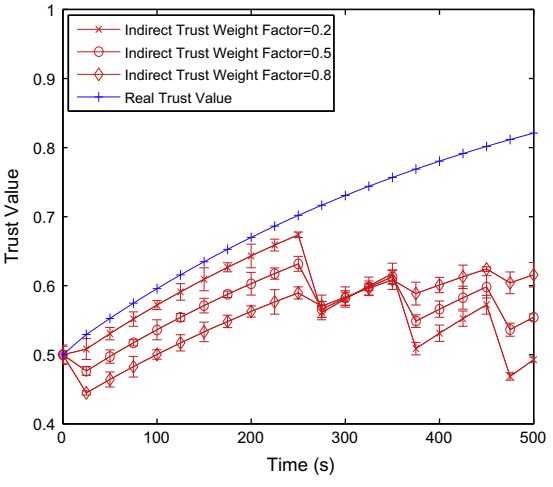


Fig. 10. The effect of IT for error detections.

7.3. The analysis of access control model

7.3.1. The access control schemes in single-domain

Compared with the conventional access model without security mechanisms, our TC-BAC may produce a certain degree of overhead owing to the trust and risk evaluation process. The effect of this kind of overhead can be considered in two respects: latency and energy consumption. In this paper, we compare TC-BAC with the other two access control models (RBAC without security considerations and the centralized authentication model). Fig. 16 indicates the different time spent on finishing the access process when adopting different models. First, we notice that the latency

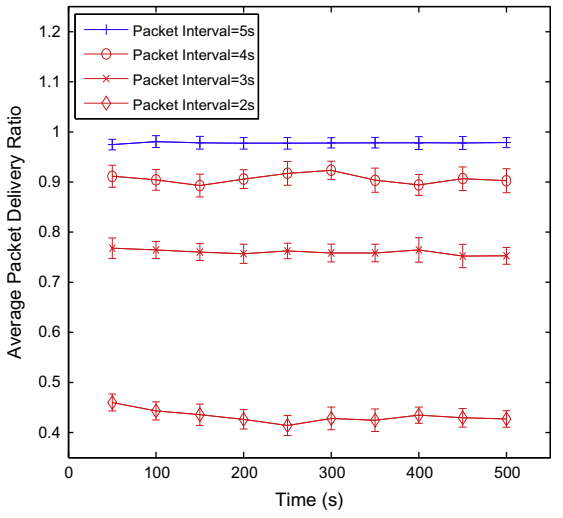


Fig. 13. The effect of network load.

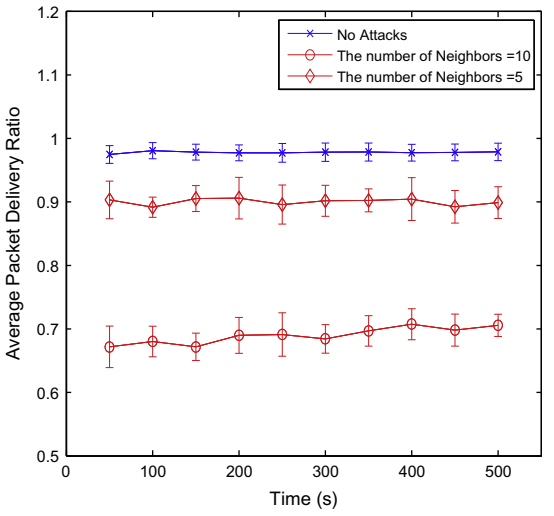


Fig. 15. The effect of node density.

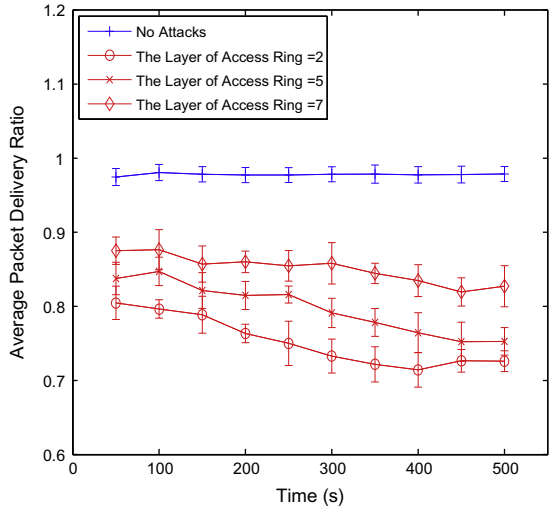


Fig. 14. The effect of access rings.

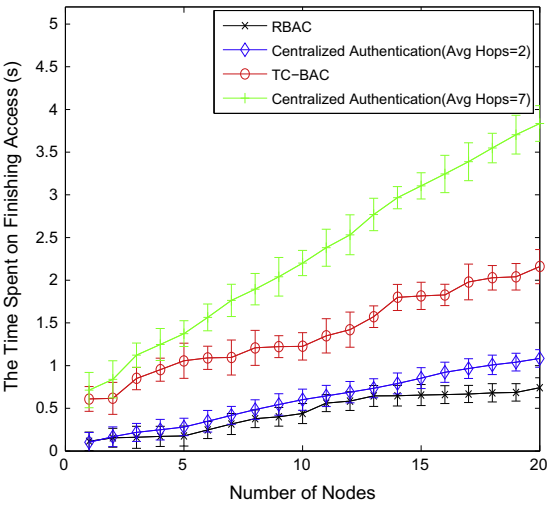


Fig. 16. The time spent on access.

of TC-BAC (about 65 ms per node) is not much higher than RBAC (about 41 ms per node) and we believe the linear increasing trend is acceptable in most cases because of the security risk. Second, we find that the performance of the centralized authentication model is affected by the hops to the central CA besides the complexity of the cryptographic primitives. As is shown in Fig. 16, the latency increases as the number of hops to the central CA increases. This situation will be more obvious when considering network congestion. Third, the latency of TC-BAC is approximately equal to the delay of the centralized authentication model with 3-hops away to the CA. Considering the multi-hop communication is one of basic features in WSNs, the latency of TC-BAC is normally acceptable.

Energy consumption is another important factor in WSNs. The model that has been used to estimate energy consumption follows the recent model proposed by Garcia-Saavedra et al. [50]. In the simulations, we pay attention to the energy consumption of the access process. From Fig. 17, we can find that the energy consumption of TC-BAC is slightly higher than RBAC. However, the extra energy consumption (about 10 J) can be negligible as compared with the total energy of the network (thousands of joules). Similarly, we also compare the energy consumption of TC-BAC with the centralized authentication model. The former mainly depends on the average number of neighbors which should provide their recommendations, while the latter depends on the average number of hops from the central CA. The energy consumption of TC-BAC (the average number of neighbors is 6) is approximately equal to the cost of the centralized authentication model with 4-hops to the CA, as shown in Fig. 17. The above simulations indicate that our access control model does not require much communication cost, and it is adaptive for the resource-constrained WSNs.

Please cite this article in press as: J. Duan et al., TC-BAC: A trust and centrality degree based access control model in wireless sensor networks, Ad Hoc Netw. (2013), http://dx.doi.org/10.1016/j.adhoc.2013.05.005

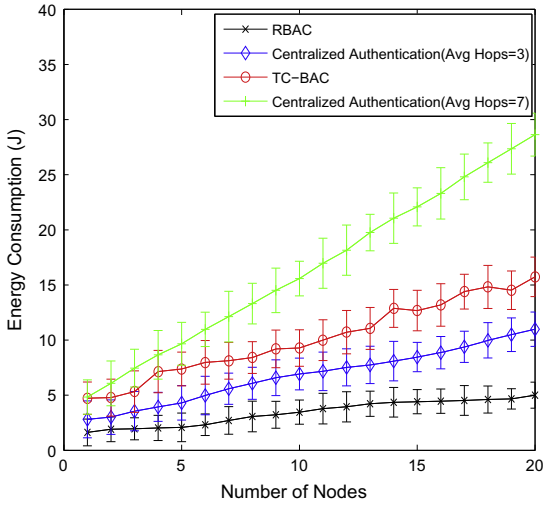


Fig. 17. The energy consumption.

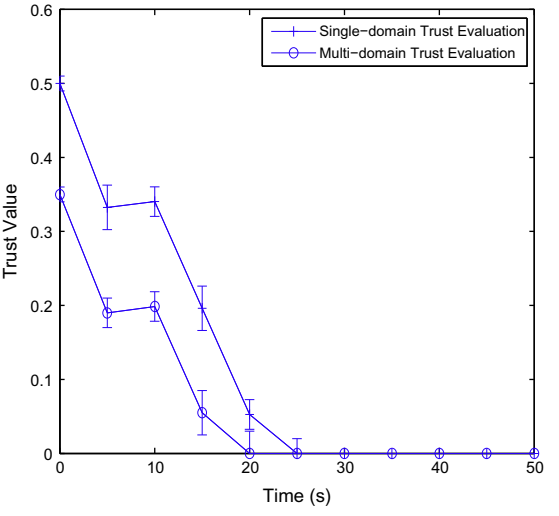


Fig. 19. The trust evaluation in the multi-domain case.

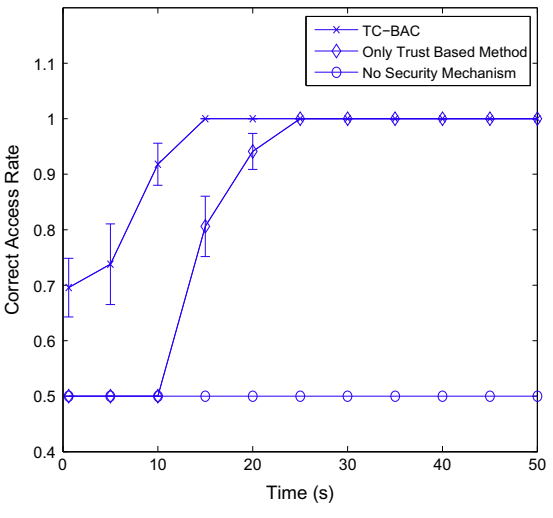


Fig. 18. The correct access rate.

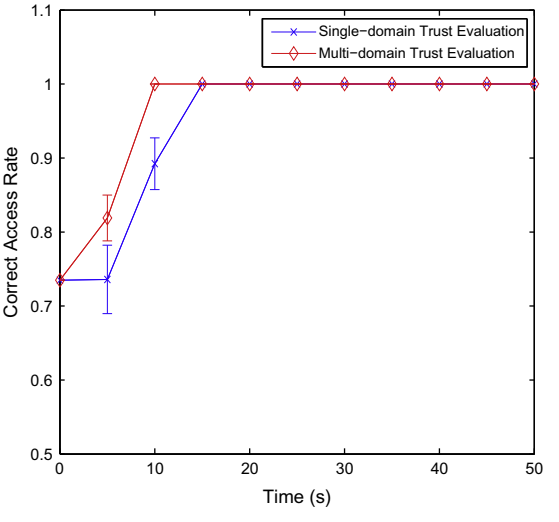


Fig. 20. The correct access rate in the multi-domain case.

To further test the robustness of the offered security features, we consider an extreme case where a number of nodes attempt to join a stable WSNs and fifty percent of them are malicious. We also define a risk threshold in the network. In this case, we will make a study of the correct access rate when adopting the TC-BAC, the only trust based access control model [46] and the conventional RBAC model respectively. As is shown in Fig. 18, the RBAC keeps fifty percent accuracy as it has no security mechanisms. The only trust based method also gets the same correct access rate at the bootstrapping time. Because there is no historical data of reference. However, the malicious nodes are gradually evicted from the network because of their bad behavior. Our TC-BAC has a mechanism of risk assessment. It is more strict about which nodes have access to the key positions of the network. Generally, the newly arriving nodes with only the initial trust value cannot join in these high risk positions, and therefore the TC-BAC always gets a higher correct access rate at the bootstrapping time. Then it has a higher probability to clear the network before the other two schemes do.

7.3.2. The access control schemes in multi-domain cases

The evaluations of the access control schemes in the multi-domain case are presented in Figs. 19 and 20. We assume that some malicious nodes in one domain try to join the other network. In the simulations, we can see that the trust evaluation process across domains can discover the malicious nodes earlier because of the mapping mechanism between the domains (about 15 s in single-domain scenarios, about 5 s in multi-domain scenarios). This mapping mechanism can effectively reduce the behavior of the

Please cite this article in press as: J. Duan et al., TC-BAC: A trust and centrality degree based access control model in wireless sensor networks, Ad Hoc Netw. (2013), http://dx.doi.org/10.1016/j.adhoc.2013.05.005

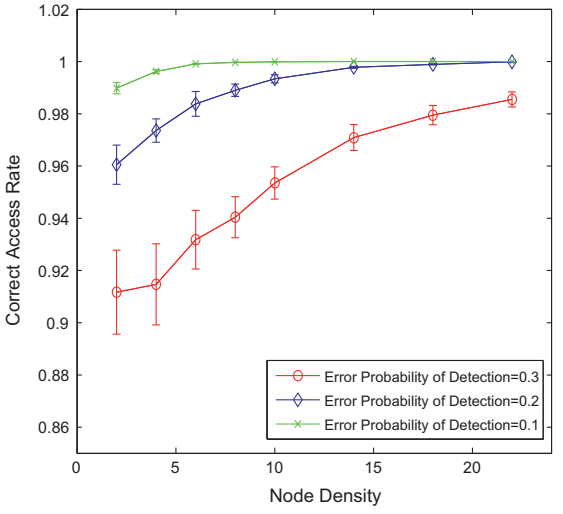


Fig. 21. The effect of error detecting on TC-BAC.

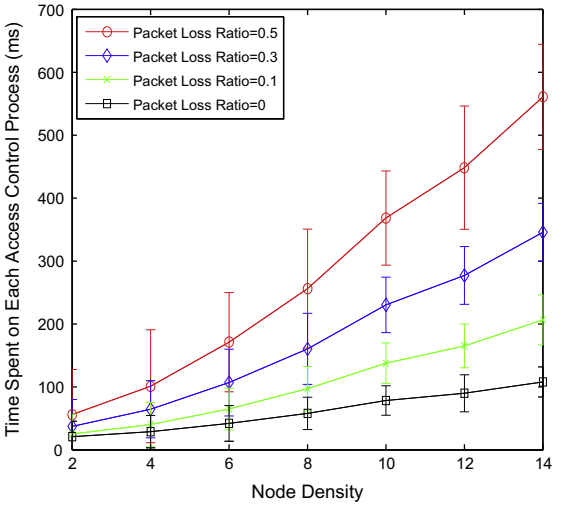


Fig. 23. The time spent on each access control process.

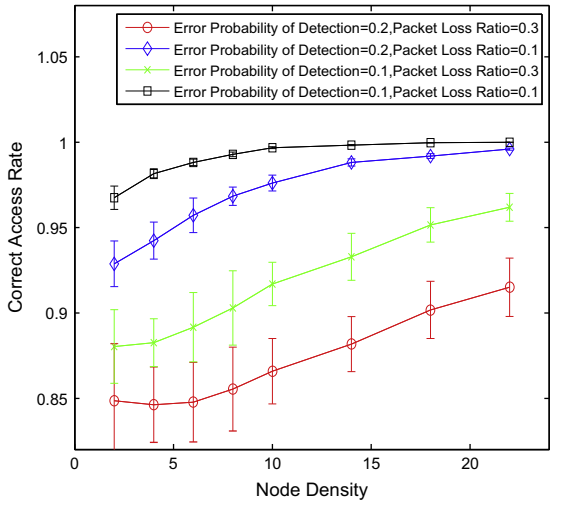


Fig. 22. The effect of packet loss ratio on TC-BAC.

malicious nodes trying to eliminate their bad reputations by joining other domains.

7.4. The applicability of TC-BAC

As WSNs are often deployed in complex environments, our proposed scheme may have different performance behaviors in different WSN setups. In this subsection, we shall focus on the impact of node density, the error probability of detection and the packet loss ratio on the performance of TC-BAC. The node density is measured by the average number of neighbors for a node. Fig. 21 first shows the accuracy of access control with different node densities and error detection probabilities. As can be seen, error probability of detection has a direct impact on the accuracy of access control. However, with an increasing node density, the accuracy of access control improves indicating that a higher node density can provide better resistance capability and reduce the adverse effect of the error detecting events. This result is in accordance with the previous simulation conclusion as the higher node density implies more recommendations in TC-BAC. Consequently, if the node density is lower than a threshold, it is possible that the required correct access rate cannot be satisfied by adopting TC-BAC.

The packet loss is a common phenomenon in WSNs, which can be caused by packet drop due to congestion, noisy channel, or node failure. As illustrated in Fig. 22, a higher packet loss ratio decreases the accuracy of access control as a high loss reduces supply of recommendation packets. Retransmission is a common method to deal with packet loss and ensures packet delivery. However, it introduces additional delay in the delivery process. Retransmission is enforced for every loss packet until the delivery is successful. In Fig. 23, we show the impact of retransmission implementation on processing time performance. The processing time increases as the node density and packet loss ratio increase. Consequently, this imposes some limitation on the support of real-time applications.

8. Conclusion and future work

In this paper, we proposed a trust and centrality-degree based access control model for WSNs. This model introduces the trust degree to evaluate the behavior of nodes in the network and utilizes the centrality degree to assess the risk factor when the new arrival nodes join the network. The simulation results show that our access control model achieves both security and efficiency.

In the future, we plan to improve the access control model so that it has the ability to provide sufficient security with lower overhead and latency. In addition, we will consider the impact of mobility on the access control process, which is a significant research point.

Please cite this article in press as: J. Duan et al., TC-BAC: A trust and centrality degree based access control model in wireless sensor networks, Ad Hoc Netw. (2013), http://dx.doi.org/10.1016/j.adhoc.2013.05.005

Acknowledgements

This work was supported by the National S&T Major Projects of China (Grant No. 2012ZX03005003), the National Natural Science Foundation of China (NSFC) (Grants No. 61272504) and the Fundamental Research Funds for the Central Universities (Grant No.2012YJS016).

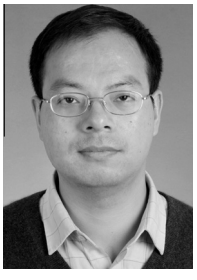
References

[1] J. Yick, B. Mukherjee, D. Ghosal, Wireless sensor network survey, Computer Networks 52 (12) (2008) 2292–2330.
[2] I. Akyildiz, I. Kasimoglu, Wireless sensor and actor networks: research challenges, Ad hoc Networks 2 (4) (2004) 351–367.
[3] T. Newman, S. Hasan, D. DePoy, T. Bose, J. Reed, Designing and deploying a building-wide cognitive radio network testbed, IEEE Communications Magazine 48 (9) (2010) 106–112.
[4] A. Cerpa, J. Elson, D. Estrin, L. Girod, M. Hamilton, J. Zhao, Habitat monitoring: application driver for wireless communications technology, ACM SIGCOMM Computer Communication Review 31 (Suppl. 2) (2001) 20–41.
[5] J.H. Cho, A. Swami, I.R. Chen, A survey on trust management for mobile ad hoc networks, IEEE Communications Surveys and Tutorials 13 (4) (2011) 562–583.
[6] D. Djenouri, L. Khelladi, N. Badache, A survey of security issues in mobile ad hoc networks, IEEE Communications Surveys 7 (4) (2005) 2–28.
[7] Y. Yu, K. Li, W. Zhou, P. Li, Trust mechanisms in wireless sensor networks: attack analysis and countermeasures, Journal of Network and Computer Applications 35 (3) (2011) 867–880.
[8] L. Yeh, Y. Chen, J. Huang, ABACS: an attribute-based access control system for emergency services over vehicular ad hoc networks, IEEE Journal on Selected Areas in Communications 29 (3) (2011) 630–643.
[9] P. Samarati, S. de Vimercati, Access control: policies, models, and mechanisms, Foundations of Security Analysis and Design 2171 (2001) 137–196.
[10] W. Xiaopeng, L. Junzhou, S. Aibo, M. Teng, Semantic access control in grid computing, in: Proceedings of 11th International Conference on Parallel and Distributed Systems, vol. 1, 2005, pp. 661–667.
[11] H. Tran, M. Hitchens, V. Varadharajan, P. Watters, A trust based access control framework for P2P file-sharing systems, in: Proceedings of the 38th Annual Hawaii International Conference on System Sciences, 2005, pp. 302c–302c.
[12] R. Yang, C. Lin, Y. Jiang, X. Chu, Trust based access control in infrastructure-centric environment, in: Proceedings of IEEE International Conference on Communications 2011 (ICC), 2011, pp. 1–5.
[13] R. Sandhu, E. Coyne, H. Feinstein, C. Youman, Role-based access control models, Computer 29 (2) (1996) 38–47.
[14] L. Abusalah, A. Khokhar, M. Guizani, A survey of secure mobile ad hoc routing protocols, IEEE Communications Surveys and Tutorials 10 (4) (2008) 78–93.
[15] S. Zhong, F. Wu, A collusion-resistant routing scheme for noncooperative wireless ad hoc networks, IEEE/ACM Transactions on Networking 18 (2) (2010) 582–595.
[16] B. Patel, D. Jinwala, Exploring homomorphic encryption in wireless sensor networks, Informatics Engineering and Information Science (2011) 400–408.
[17] S. Yu, K. Ren, W. Lou, FDAC: toward fine-grained distributed data access control in wireless sensor networks, in: Proceedings of IEEE INFOCOM 2009, 2009, pp. 963–971.
[18] S. Misra, A. Vaish, Reputation-based role assignment for role-based access control in wireless sensor networks, Computer Communications 34 (3) (2011) 281–294.
[19] H. Luo, J. Kong, P. Zerfos, S. Lu, L. Zhang, URSA: ubiquitous and robust access control for mobile ad hoc networks, IEEE/ACM Transactions on Networking 12 (6) (2004) 1049–1063.
[20] Y. Zhou, Y. Zhang, Y. Fang, Access control in wireless sensor networks, Ad Hoc Networks 5 (1) (2007) 3–13.
[21] T. Melodia, I.F. Akyildiz, Cross-layer QoS-aware communication for ultra wide band wireless multimedia sensor networks, IEEE Journal on Selected Areas in Communications 28 (5) (2010) 653–663.
[22] S. Oh, G. Marfia, M. Gerla, MANET QoS support without reservations, Security and Communication Networks 4 (3) (2011) 316–328.
[23] R.S. Sandhu, Lattice-based access control models, Computer 26 (11) (1993) 9–19.
[24] R.S. Sandhu, P. Samarati, Access control: principle and practice, IEEE Communications Magazine 32 (9) (1994) 40–48.
[25] D. Ferraiolo, R. Kuhn, Role-based access control, in: Proceedings of 15th NIST-NCSC National Computer Security Conference, Baltimore, MD, 1992, pp. 554–563.
[26] D. Ferraiolo, R. Sandhu, S. Gavrila, D. Kuhn, R. Chandramouli, Proposed NIST standard for role-based access control, ACM Transactions on Information and System Security 4 (3) (2001) 224–274.
[27] R. Zhang, Y. Zhang, K. Ren, DP^{2}AC: distributed privacy-preserving access control in sensor networks, in: Proceedings of IEEE INFOCOM 2009, 2009, pp. 1251–1259.
[28] M. Li, W. Lou, K. Ren, Data security and privacy in wireless body area networks, Wireless Communications 17 (1) (2010) 51–58.
[29] D. He, J. Bu, S. Zhu, M. Yin, Y. Gao, H. Wang, S. Chan, C. Chen, Distributed privacy-preserving access control in a single-owner multi-user sensor network, in: Proceedings of IEEE INFOCOM 2011, 2011, pp. 331–335.
[30] B. Panja, S. Madria, B. Bhargava, A role-based access in a hierarchical sensor network architecture to provide multilevel security, Computer Communications 31 (4) (2008) 793–806.
[31] R. Riggio, S. Sicari, Secure aggregation in hybrid mesh/sensor networks, in: Proceedings of 2009 International Conference on Ultra Modern Telecommunications (ICUMT), 2009, pp. 1–6.
[32] C. Gentry, A Fully Homomorphic Encryption scheme, Ph.D. Thesis, Stanford University, 2009. crypto. stanford. edu/craig (2009).
[33] S. Chakraborty, I. Ray, TrustBAC: integrating trust relationships into the RBAC model for access control in open systems, in: Proceedings of the 11th ACM Symposium on Access Control Models and Technologies, 2006, pp. 07–09.
[34] F. Almenarez, A. Marin, D. Díaz, J. Sanchez, Developing a model for trust management in pervasive devices, in: Proceedings of 4th Annual IEEE International Conference on Pervasive Computing and Communications Workshops, 2006, pp. 5–9.
[35] G. Theodorakopoulos, J. Baras, On trust models and trust evaluation metrics for ad hoc networks, IEEE Journal on Selected Areas in Communications 24 (2) (2006) 318–328.
[36] C. Zhang, X. Zhu, Y. Song, Y. Fang, A formal study of trust-based routing in wireless ad hoc networks, in: Proceedings of IEEE INFOCOM 2010, 2010, pp. 1–9.
[37] M. Mahmoud, X. Shen, Trust-based and energy-aware incentive routing protocol for multi-hop wireless networks, in: Proceedings of IEEE International Conference on Communications 2011(ICC), 2011, pp. 1–5.
[38] R. Yang, C. Lin, Y. Jiang, X. Chu, Trust based access control in infrastructure-centric environment, in: Proceedings of IEEE International Conference on Communications 2011(ICC), 2011, pp. 1–5.
[39] A. Boukerche, X. Li, An agent-based trust and reputation management scheme for wireless sensor networks, in: Proceedings of IEEE Global Telecommunications Conference 2005 (GLOBECOM), vol. 3, 2005, pp. 1857–1861.
[40] V. Karyotis, S. Papavassiliou, M. Grammatikou, On the risk-based operation of mobile attacks in wireless ad hoc networks, in: Proceedings of IEEE International Conference on Communications 2007(ICC), 2007, pp. 1130–1135.
[41] Y. Asnar, P. Giorgini, F. Massacci, N. Zannone, From trust to dependability through risk analysis, in: Proceedings of The 2nd International Conference on Availability, Reliability and Security, 2007, pp. 19–26.
[42] N. Dimmock, A. Belokosztolszki, D. Eyers, J. Bacon, K. Moody, Using trust and risk in role-based access control policies, in: Proceedings of the 9th ACM Symposium on Access Control Models and Technologies, 2004, pp. 156–162.
[43] M. Denko, T. Sun, I. Woungang, J. Rodrigues, H.-C. Chao, A trust management scheme for enhancing security in pervasive wireless networks, in: Proceedings of IEEE Global Telecommunications Conference 2009 (GLOBECOM), 2009, pp. 1–6.
[44] S. Marti, T. Giuli, K. Lai, M. Baker, et al., Mitigating routing misbehavior in mobile ad hoc networks, in: Proceedings of the 6th Annual International Conference on Mobile Computing and Networking, 2000, pp. 255–265.
[45] H. Deng, G. Jin, K. Sun, R. Xu, M. Lyell, J.A. Luke, Trust-aware in-network aggregation for wireless sensor networks, in: Proceedings of IEEE Global Telecommunications Conference 2009 (GLOBECOM), 2009, pp. 1–8.
[46] J. Luo, X. Ni, J. Yong, A trust degree based access control in grid environments, Information Sciences 179 (15) (2009) 2618–2628.
[47] K. Fall, K. Varadhan, The ns Manual, The VINT Project 1.

Please cite this article in press as: J. Duan et al., TC-BAC: A trust and centrality degree based access control model in wireless sensor networks, Ad Hoc Netw. (2013), http://dx.doi.org/10.1016/j.adhoc.2013.05.005

[48] X. Yang, D. Wetherall, T. Anderson, TVA: a DoS-limiting network architecture, IEEE/ACM Transactions on Networking 16 (6) (2008) 1267–1280.
[49] I.D. Chakeres, L. Klein-Berndt, AODVjr, AODV simplified, ACM SIGMOBILE Mobile Computing and Communications Review 6 (3) (2002) 100–101.
[50] A. Garcia-Saavedra, P. Serrano, A. Banchs, G. Bianchi, Energy consumption anatomy of 802.11 devices and its implication on modeling and design, in: Proceedings of the 8th International Conference on Emerging Networking Experiments and Technologies, 2012, pp. 169–180.

Duan Junqi received his B.S. degree in the School of Electronics and Information Engineering from Beijing Jiaotong University of China. He is a Ph.D. student in the National Engineering Laboratory for Next Generation Internet Interconnection Devices at Beijing Jiaotong University. His current research interests include security issues of wireless sensor networks and protocol design of wireless sensor networks.



Deyun Gao received B.Eng. and M.Eng. degrees in electrical engineering and a Ph.D. degree in computer science from Tianjin University, China, in 1994, 1999, and 2002, respectively. He spent 1 year as a research associate with the Department of Electrical and Electronic Engineering, Hong Kong University of Science and Technology, Kowloon. He then spent 3 years as a research fellow in the School of Computer Engineering, Nanyang Technological University, Singapore. Since 2007, he is on the faculty of Beijing Jiaotong University as an associate professor of School of Electronics and Information Engineering. His research interests are in the area of wireless sensor network, and next-generation networks.

Chuan Heng Foh received his B.Sc. in Electronic Engineering from Fu Jen Catholic University, Taiwan in 1993. During 1993–1997, he worked as a Software Engineer developing various commercial products (AS/400 Emulation Package; Voice Logging System; IVR and Voice Mail Systems, etc.). He was awarded a M.Sc. degree from Monash University, Australia in 1999 and a Ph.D. degree from the University of Melbourne, Australia in 2002. He was a Sessional Lecturer at the University of Melbourne during his Ph.D. study. He worked as a Lecturer at Monash University for 6 months in 2002. In December 2002, he joined Nanyang Technological University, Singapore as an Assistant Professor. His main interests include wireless and optical networks, mobile ad hoc networks, teletraffic, computer network modeling and performance evaluation. He has served as a member of technical program committee for many major conferences including IEEE ICC, IEEE GLOBECOM, IEEE ICCS, IEEE ICON, IEEE PIMRC, IEEE WoWMoM, and many others. He participated in organizing IFIP Networking 2008 conference. He is serving on the editorial board of the International Journal of Communications Systems (IJCS) since 2007.

Hongke Zhang received the M.S. and Ph.D. degrees in electrical and communication systems from the University of Electronic Science and Technology of China in 1988 and 1992, respectively. From September 1992 to June 1994, he was a postdoctoral research associate at Beijing Jiaotong University, and in July 1994, he became a professor there. He has published more than 100 research papers in the areas of communications, computer networks, and information theory. He is the author of eight books written in Chinese and the holder of more than 30 patents. He is now the chief scientist of a National Basic Research Program (“973” program).

Please cite this article in press as: J. Duan et al., TC-BAC: A trust and centrality degree based access control model in wireless sensor networks, Ad Hoc Netw. (2013), http://dx.doi.org/10.1016/j.adhoc.2013.05.005