19

Security architecture, trust management model with risk evaluation and node selection algorithm for WSN

Bin Ma[1,2] and Xianzhong Xie[1,2]
[1] *School of computer science and technology, Chongqing University of Posts and Telecommunications*
[2] *Institute of Personal Communications, Chongqing University of Posts and Telecommunications*
P.R. China

1. Introduction

Wireless sensor networks are ideal candidates to monitor the environment in a variety of applications such as military surveillance, forest fire monitoring, etc. In such a network, a large number of sensor nodes are deployed over a vast terrain to detect events of interest (e.g., enemy vehicles, forest fires), and deliver data reports over multihop wireless paths to the user. Security is essential for these mission-critical applications to work in an adverse or hostile environment.

Wireless Sensor networks are typically characterized by limited power supplies, low bandwidth, small memory sizes and limited energy. This leads to a very demanding environment to provide security. Public-key cryptography is too expensive to be usable, and even fast symmetric-key ciphers must be used sparingly. Communication bandwidth is extremely dear: each bit transmitted consumes about as much power as executing 800–1000 instructions(J. Hill et al 2000), and as a consequence, any message expansion caused by security mechanisms comes at significant cost.

Wireless sensor networks consist of spatially distributed autonomous devices using sensors to cooperatively monitor physical or environmental conditions, such as temperature, sound, vibration, pressure, motion or pollutants, at different locations. In addition to one or more sensor nodes, each node in wireless sensor networks is typically equipped with a radio transceiver or other wireless communication devices, a microcontroller, and an energy source, usually a battery.

Wireless sensor networks are the connection between physical world and mankind, which cannot be simply regarded as communication networks. It should mainly concentrate on sensory information processing and services. Wireless sensor networks should be developed as an integrated information infrastructure, in which information aggregation and collaborative processing are key issues.

And so, all nodes share common sensing tasks in wireless sensor networks. This implies that not all sensors are required to perform the sensing task during the whole system lifetime. Turning off some nodes does not affect the overall system function as long as there are enough working nodes to assure it. Therefore, if we can schedule sensors to work alternatively, the system lifetime can be prolonged by exploiting redundancy. In this chapter,we present a cross-layer trust management model based on cloud model; and using the trust model, we innovate an algorithm of node selection in Wireless sensor networks.
The rest of the chapter is structured as follows. In the beginning we introduce wireless sensor networks. Furthermore, A discussion of related work for security architecture and trust management model. Thereafter, we provide a unique security requirements of WSNs and present a security architecture for wireless sensor networks that addresses most of the problems above, also describe the technical aspects of our security architecture. Subsequently, we utilizes lightweight trust management model that allow for easy access control between the mobile sensor nodes and secure the communication inside the network. Furthermore, it minimizes the effects of compromised sensor nodes.

2. Related Works

2.1 security architecture

Security in sensor networks has been studied by several other researchers. Perrig et al(2001). developed the security architecture SPINS, which is based on the two protocols SNEP, a protocol for data confidentiality, two-party data authentication, and data freshness and μTESLA, a broadcast authentication protocol.Their architecture relies on the concept, that every node shares a secret key with a trusted base station, which is at all times able to communicate with every node in the network.
Furthermore, several key management schemes have been put forward for sensor networks: Basagni et al(2001). proposed a solution to periodically update a symmetric key which is shared by all nodes in the network. Their solution is based on the assumption that all nodes are constructed tamper-proof, which is not always the case. Carman et al(2000). studied several key management protocols in sensor networks with respect to performance on different hardware platforms. Zhu et al(2003). proposed the Localized Encryption and Authentication Protocol(LEAP) which utilizes four types of keys for each node. These are used for different purposes and range from the individual key that is shared with the base station, up to a group key that is shared with all nodes in the network. Eschenauer and Gligor(2002) presented a pool-based random key predistribution system, which Chan et al.(2003) extended by presenting three new mechanisms for key establishment.
Wood and Stankovic(2002,2003) identified several DoS attacks in sensor networks and presented a protocol, which allows to map regions that are subject to DoS by radio jamming.

2.2 trust management model

The traditional trust management systems are suitable for wired and wireless ad hoc network, but cannot satisfy the security requirements of wireless sensor network. Because they need very large resources consumption which is wireless sensor network lacked.
The trust management system may be the centralism or the distribution, but they both do not suit sensor network, the central system needs enough energy to satisfy the extra route need, but in the distributional system, each node needs enough storage space and strong computing

power. But in the sensor network, all node joint operation as if is more realistic. Therefore, the mix low consumption trust management system can satisfy the demand of sensor network.
Since Marsh(1994) introduced the research of trust to the computer domain, trust mechanism has gradually obtained more and more researcher's(Blaze M 1996, Adrian Perrig 2001, Sasha Slijepcevic 2002, and so on) values for its flexibility and extendibility. The people proposed the numerous trust models in distribution network, pervasive computing, peer-to-peer computing, ad hoc network and so on. In these models, trust is usually quantified as a definite real number. However, because the node trust has much subjectivity, natural insufficiency has existed by using the definite value to describe trust. For example, if node A trusts node B, it is very difficult to determine that the trust value should be 0.9 is 0.8. Therefore, uncertainty is considered to be the important attribute of trust, namely trust among the node is fuzziness and randomness; especially among strange node. Therefore, uncertainty must be considered when trust model build. Based on this, a cross-layer wireless sensor network trust model based on cloud model is proposed. This model unifies the description of trust degree and uncertainty of trust relationship among the nodes with trust cloud forms, and gives algorithms of trust cloud transmission and merge.
The cloud model by Deyi Li et al(2000,2004) has first proposed as the qualitative description and the quota expressed of one kind of terminology. It unifies the fuzziness and randomness, thus describing the uncertainty well. Now, the cloud model has already applied in numerous domains, like data mining, automatic control, quantitative evaluation and so on.

3. Security architecture

3.1 The security requirement of wireless sensor networks

Wireless sensor networks are composed of massive sensor nodes. These nodes are small, cheap, battery power supply, and have the ability of wireless communication and monitor. All the nodes are deployed densely in the monitored region to monitor the Physical world.
Because the sensor nodes mostly are deployed in the enemy or nobody region, sensor network security problem is prominent especially. Lacking effective safety mechanism already becomes the chief obstacle of the sensor network application.
Wireless sensor network's own characteristic (the limitation of computation, communication and memory, lacks of the apriority to nodes deploying, unreliable Physical security of deployed region as well as dynamic change of network topology and so on) enables the sensor network except to have the traditional network security requirements, but also has some specific security property.

Data Confidentiality

The sensor network should not reveal the information to the neighbor network. In many applications, the node transmits the highly confidential data. The standard method to protect data confidentiality is enciphered data with the key, the receiver can decipher data, therefore achieves confidentiality, establish the security channel among the nodes according to the communication mode.

Data Authentication

In the sensor network, message authentication is important to many applications. When the network is constructed, authentication to the management task is necessary. At the same

time, the enemy is very easy to insert information ,so the receivers need to determine the reliability of message's origin. The data authentication permit data confirmation that the receivers is the sender who declared sends out.
In two nodes communication, the data authentication may be achieved through the symmetrical mechanism: Sender and receiver share one key to calculate the messages authentication code (MAC) of all communication data. When the message arrived with the correct MAC, the receiver can be sure that the message indeed is the real sender sends out.

Data Integrity
In the communication, the data integrity guarantee all the data that receivers receive in transmission process not be changed by enemy. The data integrity may achieve through the data authentication.

Data Freshness
All data survey of sensor network is related with the time, cannot guarantee the confidentiality and the authentication sufficiently, but must certainly guarantee that each message is fresh. The data freshness implied the data is recent, and guaranteed that the enemy have not replay the information before. There are two types of freshness: The weak freshness provides the partial information order, but does not carry any delay information; the strong freshness provides complete order of the request/response, and permit delay forecast. The sensation survey needs the weak freshness, but in the network time synchronism needs the strong freshness.

Key management
In order to realize, satisfy the above security requirements, the encryption key needs to be managed. As a result of the energy and the computing limit, wireless sensor networks needs to maintain balanced between the security rank and these limits. Key management should include the key allocation, the initialization stage, the node increase, the key abolishment, the key renewal.
All in all, The security requirement of wireless sensor networks is main list:

1) As the key feature of wireless sensor network applications, the diversity of sensors, data flow and QoS requires the system architecture be of compatibility, universality and scalability to meet the various requirements.
2) The prevailing studies on wireless sensor networks focus on the solution of low data rate, short packet burst, low network traffic and low device energy issues. Many standardization organizations have been working on the standards of PHY/MAC layers, network protocol, identifier and sensor interfaces, however the completed security solutions on various layers have not been found out.
3) In wireless sensor network applications, such as anti-intrusion, public security, and environment monitoring, various sensors have to work cooperatively, while the current solution cannot meet the requirements.
4) The main purposes of wireless sensor networks are information sensing and processing. Thus, the security of information cooperative processing scheme in wireless sensor networks must be considered in the architecture design.

3.2 Security issues of each layers in wireless sensor networks

The network protocol stack of wireless sensor networks is composed of physical layer, data link layer, network layer, transmission layer and application layer.

Each function as follows:
Physical layer is responsible for the frequency selection, the carrier frequency production, the signal detection and the data encryption, the layer include modulation, transmission, receive and data encryption technology.
Data link layer is used for establishing communication link of reliable point-to-point or point to multipoint.
Network layer is primary responsible for route production and routing.
Transmission layer is used to establish end-to-end link between wireless sensor network and Internet or other exterior networks.
Application layer has provided kinds of practical applications of wireless sensor network.

Security problem of each layer:
Security of physical layer is how to establish the effective data encryption mechanism. Due to the property of sensor network, low expenses cryptography algorithm is still a hot spot in sensor network security research.
Data link layer or medium access control (MAC) layer provides the reliable correspondence channel for the neighbor node which is easy to come under the DOS attack. The solution is regulating the MAC admittance control, and the network neglects excessively requests automatically.
Network layer is easy to come under the attack, because each node is the latent route node, security routing algorithm immediate influence security and usability of wireless sensor network. Application layer's research mainly concentrates in providing the safe support for the entire wireless sensor network, is also the key management and the security multicast research.
Overall approach of sensor network security ensure that all layers' security, this solution could be the best option than a single security for a single layer.

3.3 Stereoscopic security architecture of wireless sensor networks

Wireless sensor network is easy to come under each kind of attack, and has many hidden security problems. At present the quite general sensor network security architecture divides the sensor network protocol stack into hardware layer, operating system layer, middleware layer and application layer. Its security module has divided into 3 layers: security primitive, security service and security application. This security architecture divided the security problem into three levels, it have the advantages of succinct question description, agreement distinctive nuance merit, but there are some general security problem among them, it could not place some security protocols in some layer to solve forcefully; And this architecture can not solve deceit of evil intention node, it have enormous hidden security problems.
With deep research on the sensor network security demand and each layer's security problem's, as well as experiences of our topic-based group, and linking the original wireless sensor network architecture, we proposed stereoscopic wireless sensor network security architecture as shown in Fig.1. This network security architecture is composed of hierarchical network communication and security protocol and the wireless sensor network support technology. The hierarchical network communication and security protocol structure is similar to the TCP/IP protocol architecture; the wireless sensor network support technology is mainly to sensor node own management as well as the user to the wireless sensor's management; two partial protocols and the technology has overlapping and the union, and have formed a cubic structural model.

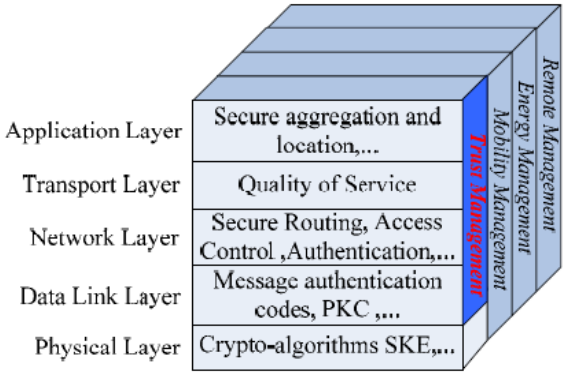


Fig. 1. security architecture of wireless sensor networks

4. Trust management model with risk evaluation

The traditional trust management systems are suitable for wired and wireless ad-hoc network, but cannot satisfy the security requirements of wireless sensor network. Because they need very large resources consumption which is wireless sensor network lacked.

The trust management system may be the centralism or the distribution, but they both do not suit sensor network, the central system needs enough energy to satisfy the extra route need, but in the distributional system, each node needs enough storage space and strong computing power. But in the sensor network, all node joint operation as if is more realistic. Therefore, the mix low consumption trust management system can satisfy the demand of sensor network.

Since Marsh introduced the research of trust to the computer domain, trust mechanism has gradually obtained more and more researcher's values for its flexibility and extendibility. The people proposed the numerous trust models in distribution network, pervasive computing, peer-to-peer computing, ad hoc network and so on. In these models, trust is usually quantified as a definite real number. However, because the node trust has much subjectivity, natural insufficiency has existed by using the definite value to describe trust. For example, if node A trusts node B, it is very difficult to determine that the trust value should be 0.9 is 0.8. Therefore, uncertainty is considered to be the important attribute of trust, namely trust among the node is fuzziness and randomness; especially among strange node. Therefore, uncertainty must be considered when trust model build. Based on this, a cross-layer wireless sensor network trust model based on cloud model is proposed. This model unifies the description of trust degree and uncertainty of trust relationship among the nodes with trust cloud forms, and gives algorithms of trust cloud transmission and merge.

The cloud model has first proposed as the qualitative description and the quota expressed of one kind of terminology. It unifies the fuzziness and randomness, thus describing the uncertainty well. Now, the cloud model has already applied in numerous domains, like data mining, automatic control, quantitative evaluation and so on.

This part of chapter uses the concept of cloud model to estimate dynamic context and consequently presents the definition of risk signal, and a trust management model based on risk evaluation for wireless sensor networks is proposed. The risk is evaluated using cloud model, quantified using risk and trust uncertainty degree are presented in a uniform form. The simulation results show that the proposed trust model based on risk evaluation can

efficiently expressed uncertainty of risk and trust, and decreased trust risk of nodes. And so this trust model also can evidently taked from the rate of trust risk, and enhanced successful cooperation ratio of WSN's system.

4.1 Cloud model

Cloud model was firstly proposed as a model of the uncertainty transition between a linguistic term of a qualitative concept and its numerical representation. In short, it is the model of the uncertainty transition between qualitative concept and quantitative description. In the discourse universe, the cloud mainly reflects two uncertainties: the fuzziness (the boundary character of both this and that) and the randomness (occurrence probability). The cloud model completely integrates the fuzziness and randomness, researches the uncertain rules which have contained by basic linguistic term(or linguistic atom) in natural language, that not only is possible to obtain the scope and distribution rule of quantitative data, but also may effectively transform precise number to qualitative linguistic term.

Formally, a cloud can be defined as follows.

Defines 1: Let U be the set as the universe of discourse, μ is a random function with a stable tendency $\mu : U \to [0,1]$,and g is also a random function with a stable tendency $g : U \to U$,He is an uncertain factor and 0…He, and

1) $u' = g(u, He), u \in U$
2) $y = \mu(u', He)$

then (U, g, μ, He) is a cloud, and (u', y) is a cloud drop.

The bell-shaped clouds, called normal clouds are most fundamental and useful in representing linguistic terms, see Fig. 2. A normal cloud is described with only three digital characteristics, expected value(Ex), entropy(En) and hyper entropy(He).

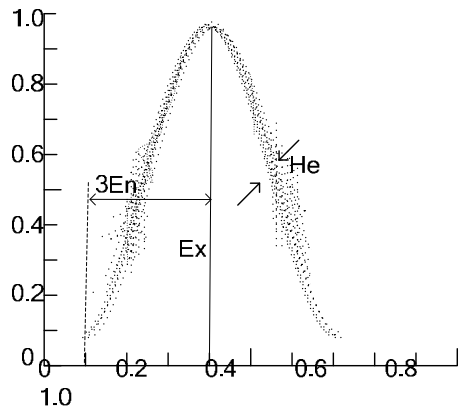


Fig. 2. Normal Cloud with digital characteristic

The expected value Ex of a cloud is the position at the universe of discourse, corresponding to the center of gravity of the cloud. In other words, the element Ex in the universe of discourse fully belongs to the linguistic term represented by the cloud model. The entropy, En, is a

measure of the fuzziness of the concept over the universe of discourse showing how many elements in the universe of discourse could be accepted to the linguistic term. It should be noticed that the entropy defined here is a generic notion, and it need not be probabilistic. The hyper entropy, He, is a measure of the uncertainty of the entropy En. Close to the waist of the cloud, corresponding to the center of gravity, cloud drops are most dispersed, while at the top and bottom the focusing is much better. The discrete degree of cloud drops depends on He.
Given three digital characteristics Ex, En, and He, to represent a linguistic term, a set of cloud drops may be generated by the following algorithm:

Algorithm 1: Forward Cloud Generator Algorithm
Input: *the expected value of cloud Ex,*
the entropy of cloud En,
the hyper entropy of cloud He,
the number of drops N.
Output: *a normal cloud with digital characteristics Ex, En, and He.*

1) *Produce a random value x which satisfies with the normal distribution probability of mean=Ex, and standard error = En;*
2) *Produce a random value En' which satisfies with the normal distribution probability of mean = En, and standard error = He;*
3) *Calculate*

$$y = \exp\left[-\left(x_i - Ex\right)^2 \Big/ 2\left(En'\right)^2 \right] \tag{1}$$

4) *Let (x, y) be a cloud drop in the universe of discourse;*
5) *Repeat 1-4 until the number of drops required all generated.*

The idea of using only three digital characteristics to generate a cloud is creative. The generator could produce as many drops of the cloud as you like (Fig. 2). This kind of generators is called a forward cloud generator. All the drops obey the properties described above. Cloud-drops may also be generated upon conditions. It is easy to set up a half-up or half-down normal cloud generator with the similar strategy, if there is a need to represent such a linguistic term. It is natural to think about the generator mechanism in an inverse way. Given a number of drops, as samples of a normal cloud, the three digital characteristics Ex, En, and He could be obtained to represent the corresponding linguistic term. This kind of cloud generators may be called backward cloud generators. Since the cloud model represents linguistic terms, the forward and backward cloud generators can be served interchangeably to bridge the gap between quantitative and qualitative knowledge.
Backward cloud gennerators are the uncertainty transformation model realizing the transformation between a numeric value and it's linguistic value, in other words, the mapping between quantitative and qualitative representation. It effectively converts a certain number of accurate data to the concept indicated by appropriate qualitative linguistic values(Ex,En,He) which represent the character of the whole drops.

In this chapter, backward cloud algorithm without certainty is adopted. The steps are presented as follows:

Algorithm 2: Backward Cloud Generator Algorithm

Input *:* $x_i(i=1,2,3...,n)$ *;*

Output *: (Ex,En,He) ;*

1) *Calculate the mean value of* x_i *,*V*、 the first order absolute central moment* M_1 *, and the variance of* x_i *,* M_2 *;*

2) *Compute the expectation of* x_i *,* $Ex = V$ *;*

3) *Compute the entropy of* x_i *,* $En = M_1 \times \sqrt{\frac{\pi}{2}}$ *;*

4) *Compute the entropy of* En *,* $He = \sqrt{M_2 - En^2}$ *。*

4.2 Trust definition

4.2.1 Risk evaluation based on cloud model

In wireless sensor network environment, entity could observe dynamic variation of context information, then feel risk. It was series approve transmit, thereof function curve too COMPare intricacy, inconvenience to with derivative 'formal description that even by surveillant dynamic context information sometimes nope series derivable, even if.Whereas uncertainty of risk, This chapter based on cloud model describe dynamic variation of context information .At known context normal state,using backward cloud algorithm without certainty protract context normal cloud, and got the digital characteristics.Compute is kept watch on the belonging to of context information sample value of time degree, if the context information that this at that time engraves samples a value to belong to normal appearance cloud and thinks to have no risk creation, whereas, think risk signal creation.The description like this even has general.

Defines 2: **context information cloud:** $Cloud = (I, t, Ex, En, He, \delta)$

Here : $I = \{S, E, C, R, U, \cdots\}$: I means aggregate of context information by watching.

t : Context information of sample partition time.

Ex : Sample point that have already known is regarded as cloud drop, we adopt the expectation value of context information cloud with the backward cloud generator. This expectation value is named the gravity of cloud. In this place, context information is accepted normal. $Ex \approx \hat{E}x = \overline{M} = \frac{1}{n}\sum_{i=1}^{n} m_i$.

En *:* The principle is above, $En \approx \hat{E}n = \sqrt{\frac{\pi}{2}} \times \frac{1}{n}\sum_{i=1}^{n} \left| m_i - \hat{E}x \right|$.

He *:* The principle is above, $He \approx \hat{H}e = \sqrt{\frac{1}{n-1}\sum_{i=1}^{n} \left(m_i - \overline{M} \right)^2 - \hat{En}^2}$.

δ : membership grade valve.

Defines 3: membership grade function definition of context information cloud, assume *m* is sampling value of context information *S* at hours *T*, and *m* that is computed by formula (2) could be known as normal degree of certainty μ :

$$\mu = e^{-\frac{(m-Ex)^2}{2(En)^2}} \tag{2}$$

$\mu > \delta$: The context information value of T time belongs to normal scope and have no risk signal creation;

$\mu < \delta$: The context information value of T time doesn't belongs to normal scope and have risk signal creation.

Above all of the risk signals is according to single context information, only with a single context information creation of the risk signal is not enough to predicate risk of occurrence in whole system. And so, we need to synthesize various risk signals of context informations to synthesize judgment.This chapter gives the evaluation method of risk.

Defines 4: definition of " Risk" : $Risk = (I', Q, \varphi)$

Here : I' is meaning that I aggregate of context information correspond with risk information

$Q = \{q_1, q_2, \cdots q_n | 0 < q_i < 1\}$: respectively representation each proportion of context information risk signal in whole sysytem.

φ : risk vavle

Risk= $S' \times q_1 + E' \times q_2 + C' \times q_3 + R' \times q_4 + \cdots > \varphi$: have risk occurrence ;

Risk= $S' \times q_1 + E' \times q_2 + C' \times q_3 + R' \times q_4 + \cdots \leq \varphi$: the context is normal and have no risk occurrence。

4.2.2 Trust cloud

Trust cloud is the core concept of the model. Based on the formalized definition of the cloud, its formalized definition is given as follows:

Defines 5: The trust cloud is the description of trust relationship among nodes with One-Dimensional Normal Cloud forms, it indicates is:

$$\left.\begin{array}{c} tc_{AB} = nc(\mathrm{Ex}, \mathrm{En}, \mathrm{He}, \mathrm{Risk}) \\ 0 \leq \mathrm{Ex} \leq 1, 0 \leq \mathrm{En} \leq 1 \\ 0 \leq \mathrm{He} \leq 1, 0 \leq Risk \leq 1 \end{array}\right\} \tag{3}$$

That is, trust is a normal cloud among the nodes, Ex is trusts expectation., it indicates basic trust value of node A to the B; En is trust entropy, it reflects uncertainty of the trust relationship; He is trust ultra entropy, it reflects uncertainty of the trust entropy; and Risk is trust risk, it reflects degree of trust risk.

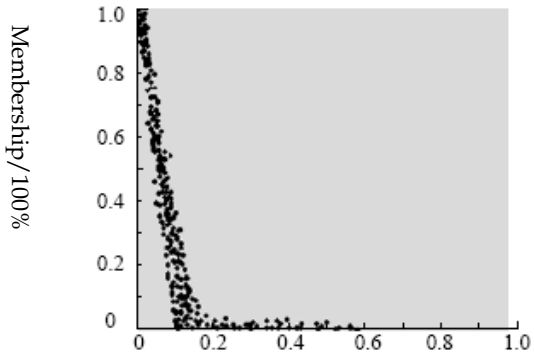
It must point out that when En is close to 0 and He=0, trust relationship among the nodes is fuzzy, but its ambiguity is definite. When En=0 and He=0, trust relationship among the nodes is definite and have no uncertainty. For example, the node is interior node of the system or definite trust relationship in the identical management system. In the chart 4-1, several different shapes of trust cloud have been given, and they have represented different trust value and uncertainty separately. Discovered from the chart that Ex is bigger, the trust cloud is closer to the biggest trust value, namely 1; En is bigger, the trust cloud's scope is wider; He is bigger, the trust cloud's cloud drop dispersion is bigger.

4.2.3 Differences between distrust and unknown trust

In the trust model, distrust and unknown trust has the difference. If node A does not trust node B, it represents A know B, and cannot trust it. However, if node A unknown trust node B, it represents A not know whether should trust B. The tradition method is using different trust value to distinguish distrust and unknown trust. For example: - 1 describes unknown trust and 0 describes distrust. However, this cannot reflect two concepts truthfully, especially unknown trust.

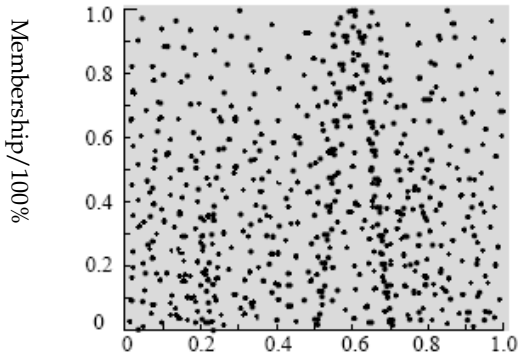
In the view of cloud model, distrust describe trust relationship among the nodes from the trust value angle, might use Ex=0 to describe. The unknown trust describe trust relationship among the nodes from trust uncertainty angle, may use En=1 and He=1 to describe.

However, these two kinds of trust have the possibility to coexist in the identical trust relationship. For example: If node A is strange to node B, therefore B unknown trusts A. Suppose B's trust threshold is small, A will be trusted under the certain extent. On the contrary, Suppose B's trust threshold is big, B will not trust A. In this case, the existing trust model could not describe. Based on the cloud model trust model distrust can be described by establishment expectation Ex =0 and unknown trust can be described by establishes ultra entropy En. From Fig. 3 (a) ~ (d), it can be seen that distrust and unknown trust have the differences of definiteness and the uncertainty as well as have the possibility to overlap.



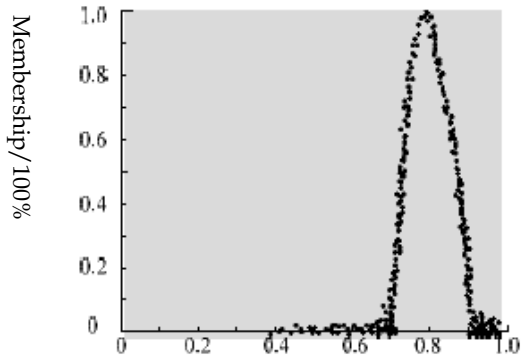
tc(0,0.05,0.001)

(a) Somewhat definite distrust



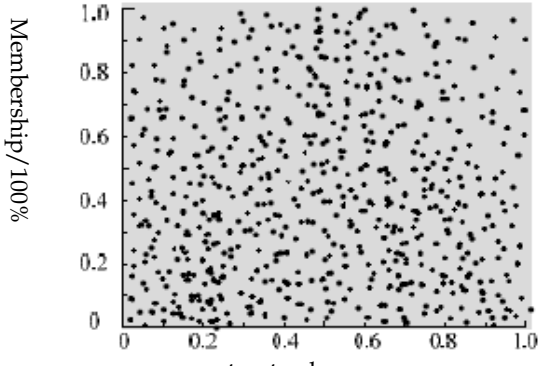
tc(0.6,0.1,0.2)

(b) Somewhat uncertainty unknown trust



tc(0.8,0.1,0.001)

(c) Somewhat indefinite distrust



tc(0.01,0.1,0.3)

(d) unknown trust, also distrust

Fig. 3. distrust and unknown trust cloud chart

4.3 Trust Propagation

In the wireless sensor network, the node cannot always directly obtain the recommendation trust value of the strange node from the neighbor node, therefore trust propagation is introduced. Supposed there are m nodes as E1, E2, E3, …Em, the node Ei, Ei+1($0 \le i \le m-1$) have the trust cloud $tc_i(Ex_i, En_i, He_i)$,and then computing the cloud trust $tc(Ex, En, He)$ is needed by this.

Because the trust cloud of E1 to Em is transmitted by the middle nodes, this is called trust cloud's propagation, and its computation algorithm is as follows:

$$\left.\begin{aligned} tc\left(\mathrm{Ex},\mathrm{En},\mathrm{He},\mathrm{Risk}\right) &= tc_1 \otimes tc_2 \otimes \cdots \otimes tc_m \\ &= \prod_{i=1}^{m} tc_i\left(\mathrm{Ex_i},\mathrm{En_i},\mathrm{He_i},Risk_i\right) \\ \mathrm{Ex} = \prod_{i=1}^{m} \mathrm{Ex_i},\ \mathrm{En} &= \min\left(\sqrt{\sum_{i=1}^{m} \mathrm{En_i^2}},1\right) \\ \mathrm{He} = \min\left(\sum_{i=1}^{m} \mathrm{He_i},1\right),\ Risk &= \min\left(\sum_{i=1}^{m} Risk_i,1\right) \end{aligned}\right\} \tag{4}$$

Here $\otimes$ is called as trust cloud logical multiplication operator. Analyze the parameter's significance, the trust cloud expectation more draws close to 0, the ultra entropy that the cloud drop dispersion increases, obviously after propagation, trust cloud's trust degree reduces with the uncertainty increases, this in accordance with the actual situation.

4.4 Trust mergence

In the wireless sensor network, the trust relationship during the numerous nodes constituted a trust network, there are many trust ways between two nodes. Thus, according to different trust ways, when calculating the trust relationships between two nodes it will obtain many trust clouds. By now, these clouds need to merge a trust cloud.

Supposed there are m nodes as $tc_1, tc_2, tc_3, \ldots, tc_m$, the nodes may merge into a trust cloud by the algorithm as follows:

$$\left.\begin{aligned} tc\left(\mathrm{Ex},\mathrm{En},\mathrm{He},\mathrm{Risk}\right) &= tc_1 \oplus tc_2 \oplus \cdots \oplus tc_m \\ &= \sum_{i=1}^{m} nc_i\left(\mathrm{Ex_i},\mathrm{En_i},\mathrm{He_i},Risk_i\right) \\ \mathrm{Ex} = \frac{1}{m}\prod_{i=1}^{m} \mathrm{Ex_i},\ \mathrm{En} &= \min\left(\frac{1}{m}\sum_{\mathrm{i}=1}^{\mathrm{m}} \mathrm{En_i},1\right) \\ \mathrm{He} = \min\left(\frac{1}{m}\sum_{i=1}^{m} \mathrm{He_i},1\right),\ Risk &= \min\left(\frac{1}{m}\sum_{i=1}^{m} Risk_i,1\right) \end{aligned}\right\} \tag{5}$$

Here $\oplus$ is called as the trust cloud logical add operator. Analyze the parameter's significance, the cloud trust degree and the uncertainty of the merged cloud must surpass the first two kind of trust cloud.

5. Node selection algorithm for WSN

In this trust model, trust is not indicated with any definite value, but uses the trust cloud to express. The trust cloud is described with three digital eigenvalue, for it's very difficult to apply the trust cloud directly. Therefore, when selects node, using a definite trust value is quite important. In this model, a trust factor is defined. The trust factor can be calculated by using trust cloud and node can be chose with the trust factor.

5.1 calculates trust factor

Because this trust model describes trust with cloud, it not only described the trust degree moreover to describe trust indefiniteness, the definition algorithm of computation trust factor has also manifested these two characteristics. Therefore algorithm of trusted factor computation has defined as follows:

Supposed a trust cloud $tc(Ex, En, He)$ and N cloud drops, the trust factor can be calculated as the following steps:

- generate N cloud drop according to the forward cloud generator algorithm
- Calculates the trust factor with the formula

$$tg = \frac{1}{N}\sum_{i=1}^{N} x_i \times y_i \tag{6}$$

As the above algorithm shown, influenced by normal random number of the forward cloud generator algorithm, the calculated trust factor can not be the same by many times, this has also manifested the trust uncertainty. However, there will still be a trust expectation. If the trust cloud using En=0 and He=0 to describes a definite trust, the factor will present the same value every time when calculated it, namely Ex.

5.2 node selection algorithm

The processing flow of wireless sensor node selection algorithm as follows.

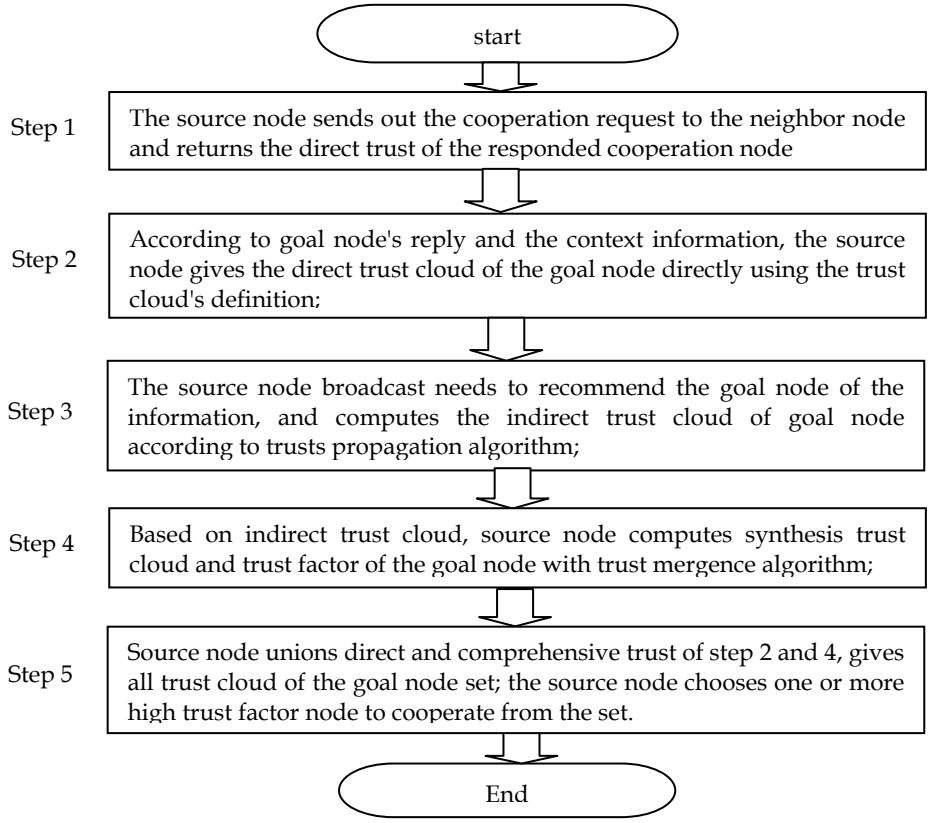


Fig. 4. wireless sensor node selection algorithm

6. Conclusion and Further Research

In this chapter, we have proposed a security architecture that provides confidentiality, integrity, and authentication with trust management for a wireless sensor network. For this purpose, we present a security architecture for wireless sensor networks that addresses most of the security requirements. It utilizes lightweight trust model algorithms that allow for easy acess control between the mobile sensor nodes and secure the communication inside the network. Furthermore, it minimizes the effects of compromised sensor nodes.Finally, we propose a cross-layer wireless sensor network trust model based on cloud model. This model unifies the description of trust degree and uncertainty of trust relationship among the nodes with trust cloud forms, and gives algorithms of trust cloud transmission and merge. By using the trust model and algorithm, a Node selection algorithm based on trust cloud is proposed.

7. Acknowledgements

This research work has been partially supported by the National Natural Sciemce Foundation of China under grant No.60872037, the Science & Technology Research Program of the Municipal Education Commission of Chongqing of China under Grant No. KJ090506, and the Natural Science Foundation of Chongqing of China under Grant No. CSTC 2010BB2218, CSTC 2008BB2411.

8. References

A.Cerpa, J.Elson, D.Estrin, L.Girod,M.Hamilton and J. Zhao.(2002)Habitat Monitoring: Application Driver for Wireless Communications Technology,*UCLA Computer Science Technical Report*.

Anderson, R., and Kuhn, M.(1996). Tamper Resistance – A Cautionary Note. *Proceedings of the 2nd Usenix Workshop on Electronic ommerce*, pp.1-11, USENIX Association, Oakland.

Basagni, S., Herrin, C., Bruschi, D., and Rosti, E.(2001). Secure Pebblenets. *Proceedings of the 2nd International Symposium on Mobile Ad Hoc Networking & Computing*.pp. 156 – 163, ACM Press, Washington DC.

Bin Ma.(2009).A Novel Stereoscopic Security Architecture with Trust Management for Wireless Sensor Networks.*Proceedings of the ICCSN '09*. pp.797-800, IEEE Computer Society Press,Maoco.

Bin Ma.(2009).Cross-Layer Trust Model and Algorithm of Node Selection in Wireless Sensor Networks.*Proceedings of the ICCSN '09*. pp.812-815, IEEE Computer Society Press,Maoco.

Blaze M, Feigenbaum J, Lacy J.(1996). Decentralized trust management. *Proc. of the 17th Symp. on Security and Privacy*. pp.164−173.Oakland: IEEE Computer Society Press.

Carman, D.W., Kruus, P.S., and Matt, B.J.(2000). *Constraints an Approaches for Distributed Sensor Network Security*. Technical Report, NAI Labs.

Chan, H., Perrig, A., and Song, D.(2003).Predistribution Schemes for Sensor Networks. *Proceedings of the IEEE Security and Privacy Symposium*.pp. 197 – 213. IEEE Computer Society Press, Los Alamos.

Deyi Li,Changyu Liu,Yi Du,Xu Han.(2004). Artificial Intelligence with Uncertainty. *Journal of Software*, vol. 15(11),pp 1583-1594.

Deyi Li.(2000). Uncertainty in Knowledge Representation. *Engineering Science*, vol. 2(10),pp 73-79.

Eschenauer, L., and Gligor, V.D.(2002).A Key-Management Scheme for Distributed Sensor Networks. *Proceedings of the Conference on Computer and Communications Security '02*. pp. 41 – 47.Washington DC .

I.F.Akyildiz, W.Su, Y.Sankarasubramaniam, E.Cayirci.(2002). Wireless Sensor Networks: A Survey, *Computer Networks*,Vol. 38, No. 8, August 2002, pp. 398-422.

J. Hill, R. Szewczyk, A. Woo, S. Hollar, D. Culler and K. Pister. (2000). System architecture directions for networked sensors. *Proceedings of ACM ASPLOS-IX*,pp.21-28, Cambridge,MA,USA.

J. Kahn, R. Katz, and K. Pister.(1999).Next Century Challenges: Mobile Networking for Smart Dust, *Proc. of ACM MobiCom'99*,pp. 271-278.ACM Press, Washington DC.

Ma Bin.(2008). Coordinated Trust Model in Pervasive Computing Based on Cloud Theory. *Computer Engineering*, vol. 34(9),pp 162-163,166.

Ma Bin,Xie Xian-zhong.(2009). A novel intelligent risk based access control planning. *Journal of Chongqing University of Posts and Telecommunications(Natural Science Edition)*, vol. 21(4),pp 523-527.

Ma Bin,Xie Xian-zhong.(2010). Cloud Trust Model for Wireless Sensor Networks. *Computer Science*, vol. 37(3),pp 128-132.

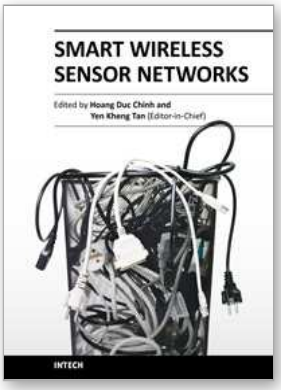
Perrig, A., Szewczyk, R., Wen, V., Culler, D., and Tygar, J.D.(2001). SPINS: Security Protocols for Sensor Networks. *Proceedings of the 7th International Conference on mobile Computing and Networks*.,pp.189 –199,ACM Press, Washington DC.

S. Marsh.(1994) Formalising Trust as a Computational Concept, *Departmet of Computer Science and Mathematics of PhD: University of Stirling*.

Wood, A.D., and Stankovic, J.A.(2002). Denial of Service in Sensor Networks.*IEEE Computer*, Vol. 35, No. 10, October 2002, pp. 54 – 62.

Wood, A.D., Stankovic, J.A, and Son, S.H.(2003). JAM: A Jammed-Area Mapping Service for Sensor Networks. *Proceedings of the 24th Real-Time Systems Symposium*.pp. 286 – 297. IEEE Computer Society Press, Los Alamos .

Zhu, S., Setia, S., and Jajodia, S.(2003).LEAP: Efficient Security Mechanisms for Large-Scale Distributed Sensor Networks.*Proceedings of the Conference on Computer and Communications Security '03*.pp. 62 – 72, ACM Press, Washington DC, 2003.



Smart Wireless Sensor Networks

Edited by Yen Kheng Tan

ISBN 978-953-307-261-6
Hard cover, 418 pages
Publisher InTech
Published online 14, December, 2010
Published in print edition December, 2010

The recent development of communication and sensor technology results in the growth of a new attractive and challenging area â€“ wireless sensor networks (WSNs). A wireless sensor network which consists of a large number of sensor nodes is deployed in environmental fields to serve various applications. Facilitated with the ability of wireless communication and intelligent computation, these nodes become smart sensors which do not only perceive ambient physical parameters but also be able to process information, cooperate with each other and self-organize into the network. These new features assist the sensor nodes as well as the network to operate more efficiently in terms of both data acquisition and energy consumption. Special purposes of the applications require design and operation of WSNs different from conventional networks such as the internet. The network design must take into account of the objectives of specific applications. The nature of deployed environment must be considered. The limited of sensor nodesâ€™ resources such as memory, computational ability, communication bandwidth and energy source are the challenges in network design. A smart wireless sensor network must be able to deal with these constraints as well as to guarantee the connectivity, coverage, reliability and security of networkâ€™s operation for a maximized lifetime. This book discusses various aspects of designing such smart wireless sensor networks. Main topics includes: design methodologies, network protocols and algorithms, quality of service management, coverage optimization, time synchronization and security techniques for sensor networks.

How to reference

In order to correctly reference this scholarly work, feel free to copy and paste the following:

Bin Ma and Xianzhong Xie (2010). Security Architecture, Trust Management Model with Risk Evaluation and Node Selection Algorithm for WSN, Smart Wireless Sensor Networks, Yen Kheng Tan (Ed.), ISBN: 978-953-307-261-6, InTech, Available from: http://www.intechopen.com/books/smart-wireless-sensor-networks/security-architecture-trust-management-model-with-risk-evaluation-and-node-selection-algorithm-for-w

INTECH
open science | open minds

InTech Europe
University Campus STeP Ri
Slavka Krautzeka 83/A
51000 Rijeka, Croatia

InTech China
Unit 405, Office Block, Hotel Equatorial Shanghai
No.65, Yan An Road (West), Shanghai, 200040, China
中国上海市延安西路65号上海国际贵都大饭店办公楼405单元

Phone: +385 (51) 770 447
Fax: +385 (51) 686 166
www.intechopen.com

Phone: +86-21-62489820
Fax: +86-21-62489821