Indonesian Journal of Electrical Engineering and Computer Science
Vol. 4, No. 1, October 2016, pp. 141 ~ 147
DOI: 10.11591/ijeecs.v4.i1.pp141-147

An Energy-Efficient Key Management Scheme using Trust Model for Wireless Sensor Network

P. Raja*, E. Karthikeyan
Department of Electronics and Communication Engineering, Sri Manakula Vinayagar Engineering College, Puducherry, India
*Corresponding author, e-mail: rajashruthy@gmail.com

Abstract

In wireless sensor networks (WSNs), secret shared keys must be established with the neighboring nodes in order to achieve secure communication. The challenge issues for secured communication in WSN are the Key management. Location Dependent Key (LDK) management is a suitable scheme when compared to other location based key management schemes because of lesser memory space requirement and lesser number of keys to be stored on each sensor node. However, the LDK is affected by communication interference problem which is solved by the key is distributed based on trust model. The distributed key updates and revocation processes are effectively resist inside attackers. An energy-efficient Key Management with Trust Model (KM-TM) for WSNs is proposed to achieve the secured communication and the nodes are resisting from the attackers. The performances of proposed KM-TM for WSNs are evaluated in terms of trustworthiness of sensor nodes and security breaches more effectively.

Keywords*: Wireless sensor network, location dependent key management, trust model*

1. Introduction

Wireless sensor networks (WSNs) consist of number of wireless Sensor Nodes (SNs) that operate without centralized control and fixed infrastructure. Since there is no fixed infrastructure, therefore the sensor nodes are deployed in any scenario [1]. The sensor nodes are communicated the sensed information to the sink node wirelessly, therefore, it is more vulnerable to attacks. These attacks have a great impact on applications such as battlefield spying and environment monitoring. The malicious nodes can introduce active intrusion, passive eavesdropping, and modification of original information and flooding of message in the network. In passive eavesdropping, the attacker hacks the private information. In active intrusion, the attacker can delete the original information, modify the information or include some false information to the original message. Thus, providing security is an important issue in WSNs.

To avoid security threats, various security mechanisms such as cryptography [2], message integrity [3], authentication and confidentiality [4] have been proposed. Unfortunately, the available complex encryption algorithms [5] are not suitable for WSNs due to the restricted capabilities of nodes. Hence, it is required to select the adoptable symmetric cryptographic method.

With the protection of cryptographic method, the compromised authenticated nodes are unable to determine the threat while using intrusion detection and prevention schemes. The adversaries or attackers take the control of the network if the compromised nodes in the network are not identified in time and so that the adversaries can seize the secret information. Hence, it is necessary to propose an efficient scheme in order to identify the compromised nodes in time and to reduce the loss in the network.

A key management is required when employing cryptographic schemes. For secure communication between two entities, a secret key should be employed [6]. There are two possible ways for secure communication. One is the entities concerned to share a single key, which is known as symmetric key system, and another one is for the entities concerned to share different keys, which are known as asymmetric key system [7-9]. These key are distributed in the network and they are updated when required, erased if the keys are compromised.

Received May 13, 2016; Revised August 16, 2016; Accepted September 1, 2016

In this paper, an energy-efficient Key Management scheme using Trust Model (KM-TM) is proposed for WSNs, which is used to prevent the security breaches effectively and to compute the trustworthiness of sensor nodes. The simulation results show that the proposed KM-TM model outperforms the existing LDK+.

2. Related Work

In WSN, sensor nodes perform wireless communication with the help of neighbor nodes. WSN is not only used to measure environmental conditions such as temperature and sound, but also used to gather sensitive data [10]. All communications should be carried out securely in order to prevent privacy issues.

By 2020, the Internet of Things (IoT) which leads to a high economic value [9] which connects 26 billion devices and used in secured applications such as military, medicine, industry and traffic, etc., [11]. Since WSN uses actual data, security plays a vital role in the study of WSNs [12]. General security techniques such as authentication and authorization cannot detect insider attackers. Hence, insider threats are one of the critical security factors in WSN. This threat creates a great impact on applications such as military surveillance systems.

Eschenauer and Gligor [13] describe the key management schemes. The key management schemes are classified into pair-wise key management, pre-distributed random key management and location-based key management. The factors such as efficiency, scalability and heterogeneity are the main objectives of this key management because of the hardware restrictions of sensor networks.

In WSN key management, location based key management is a core part of the research. SN should be located in an assigned grid in grid based key management. It is difficult to locate SNs in an assigned grid when sensor networks are used for the detection of an enemy in a military zone. Anjum's scheme depends only on the location of SNs without considering the information about the deployment [14]. This scheme considers only the insider threads to WSN in order to develop the key management technique.

Location based key (LDK+) management scheme is proposed in [15]. LDK+ is the key establishment process using Anchor Nodes (ANs) based on LDK. In this scheme, the key is generated and updated to provide security to the network. The key revision phase from a neighbor node is included as like LDK, each SN equipped with pre-deployment keys. The key generation consists of three phases. They are:

1. Pre-deployment phase
2. Initialization phase
3. Key establishment phase

Pre-deployment phase: In the pre-distribution phase, before deployment SNs saves the information required to generate the key called as pre-deployment keys.

Initialization phase: In the initialization phase, AN transmits nonces to SNs at different power levels. SNs receive nonces based on the location of SNs.

Key establishment phase: In the key establishment phase, the key is generated based on the combination of pre-deployment key and received set of nonces. The key generation of SNs is location dependent. The SNs which are not in similar location receives different set of nonces due to which resulting keys are different.

3. Proposed Method

To improve the performance of LDK+ in terms of energy and security, trust model is used and named as Key Management using Trust Model (KM-TM). Trust model is used to reduce the energy consumption and total node death because that the key is shared only between the trusted nodes and to improve connectivity, since the key distribution takes place in the trusted path. In Trust Model for WSNs, direct and recommendation trusts are evaluated based on the number of packets that the sensor nodes received. Then, during the calculation of direct trust, communication, energy and data trusts are considered. In the existing research field, the trust values of SNs are assessed based on the communication point of view. The decision of trusted sensor node is not only depend on communication behavior but also required to consider another trust metric like energy level in order to compute the

trustworthiness of SNs. Due to the noise over communication channel and behavior of unstable SNs, an uncertainty occurs. Hence, it should be taken into account for an efficient trust model.

3.1. Trust Model

The trust model is established by two ways for WSN. The first way is that direct trust value is calculated based on the direct interactions and the second way is that based on the recommendation from the third party, the indirect trust value is calculated. It is required to analyze the third party, recommendation since not all the third parties is trusted, and not all the recommendations are reliable. Most of the existing work requires accessing the trust value of neighbor nodes. However, in real applications it is necessary to obtain the trust value of non-neighbor nodes. The trust relationship between SNs may constantly vary, due to the dynamic topology. The trust dynamic problem is not solved by most of the existing trust models. The proposed trust model is used to solve the aforementioned problems. The trust relationship between SNs is evaluated precisely and the security breaches can be prevented effectively.

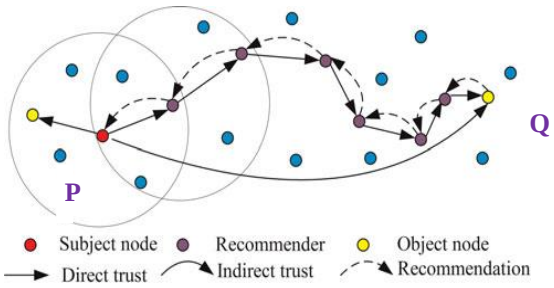

Figure 1. Network Structure [16]

In trust model, the fixed SNs are randomly deployed as shown in Figure 1, there are three types of nodes such as subject, recommender and object nodes. If a sensor node *P* needs to compute the trust value of sensor node *Q*, then sensor node *P* is referred as subject node and the sensor node *Q* is referred as the object node. The subject nodes communicated directly with the neighbor nodes within their communication range. The non-neighbor nodes exchanges the packet between them and the packets are forwarded by other nodes in the network. The main function of the forwarding node is not only transfer or pass the packets from source to destination process depend upon their own judgments. Based on the observation of subject node on the object node and third party recommendations, the trust value is calculated. The third party that provides recommendations to find trust value is referred as recommender.

Calculation of Direct Trust: Direct trust can be composed by considering the communication, energy and data trusts. In WSNs, the SNs usually co-operate and interact with neighbor nodes to perform their functions. Therefore, in order to evaluate whether the sensor node is normal or not, the communication behaviors of the sensor nodes are always checked. The data overflow between sensor nodes is unstable because of wireless communication. Malicious nodes or unstable communication channel may cause the unsuccessful communication. Therefore, evaluating the communication behaviors is not sufficient for trust evaluation. To transmit the data packets or any information will consume certain amount of energy of the sensor node. In WSNs, the malicious nodes will consume abnormal energy or the transmitted data packets will be dropped by malicious attacks. The communication trust exists if a sensor node can cooperatively execute the intended protocol. To measure that if a sensor node is capable of performing its assigned functions or not energy trust is used. The data trust is the trust assessment of trust over fault tolerance and consistency of data, such that the trust of the sensor nodes will be affected that create and handle the data.

Calculation of Communication Trust: Communication trust is calculated based on the information on a sensor node's previous communication behavior. In WSNs, due to unstable and noisy communication channels between two SNs, the behaviors of sensor node's is monitored depend on previous communication behaviors involves considerable uncertainty [16]. The trust value based on Subjective Logic (SL) frame work [18] is a triplet T = {b, d, u}, where b,

d and u correspond to belief, disbelief and uncertainty respectively. Based on the successful (s) and unsuccessful (f) communication packets, the communication trust is calculated by:

$$T_{com} = \frac{2b + u}{2} \quad (1)$$

Where $b = \frac{s}{s + f + 1}$ and $u = \frac{1}{s + f + 1}$.

Calculation of Energy Trust: In WSNs, energy is one of the important metrics because sensors nodes are depend on the amount of energy. Malicious nodes are launching malicious attacks by consuming abnormal energy. To measure whether a sensor node is selfish or maliciously exhaust additional energy, energy is used as a QOS trust metric. The energy consumption of sensor nodes in several periods is obtained by using an energy prediction model.

Initially, an energy threshold θ is defined. If the residual energy (E_{res}) of SN falls below the defined threshold value, then the SNs do not have enough energy to perform the assigned function. Hence, the energy trust is considered zero for that particular sensor node. Based on the energy consumption rate (p_{ene}), the energy trust is computed where $p_{ene} \in [0,1]$. If the energy consumption rate is higher, then the residual energy remains less which leads to smaller ability of sensor nodes to finish the task. Hence, the trust values of the sensor nodes are considered as small. The energy trust is calculated by:

$$T_{ene} = \begin{cases} 1 - p_{ene}, & if\ E_{res} \geq \theta \\ 0, & else \end{cases} \quad (2)$$

Where p_{ene} is calculated by ray projection method [19].

Calculation of Data Trust: The trust of the data affects the trust of the network nodes that created and manipulated the data, and vice-versa [20]. The data packets have spatial correlation, that is, the packets sent among neighbor nodes are always similar in the same area. The data value of these packets in general follows some certain distribution, such as a normal distribution. For a set of data, the probability density function is f(x), where x is the attribute value v_d of a data item, and μ and σ are mean and variance of the data, respectively. For the sake of simplicity, the distribution of the data is modeled as a normal distribution. Since the mean μ of a set of data is the most representative value that reflects the value similarity of the data, the mean is supposed to have the highest trust value. If the value of a data item is close to the mean, the trust value of this data is relatively high, and vice-versa. Therefore, the trust value of the data item is defined as [21]:

$$T_{data} = 2(0.5 - \int_{\mu}^{v_d} f(x)\,dx = 2\int_{v_d}^{\infty} f(x)\,dx \quad (3)$$

Based on the communication trust T_{com}, the energy trust T_{ene} and the data trust T_{data}, we can obtain the direct trust between two neighbor nodes as:

$$T_{n-direct} = w_{com}T_{com} + w_{ene}T_{ene} + w_{data}T_{data} \quad (4)$$

Where w_{com}, w_{ene} and w_{data} are the weight values of the communication trust, energy trust and data trust respectively, $w_{com} \in [0, 1]$, $w_{ene} \in [0, 1]$, $w_{data} \in [0, 1]$ and $w_{com} + w_{ene} + w_{data} = 1$.

4. Results and Discussion

The simulation environment created for the network size of 100 × 100 m^2, which consists of number of 100 sensor nodes. The simulation parameters are shown in Table 1 are

used to evaluate the performance of KM-TM. The performance KM-TM was evaluated using MATLAB in terms of residual energy, node death, connectivity and mean square error and compared with the existing key management scheme.

The following performance metrics are considered to evaluate the efficiency of the network.

1. *Residual energy:* It is defined as the remaining energy of the sensor network.
2. *Node death rate:* It demonstrates number of alive nodes over rounds. A lower node death rate happens because of load balanced network.
3. *Connectivity:* Connectivity of a node is defined as the ratio of the number of neighbors of the node with which it can form secure links to the total number of neighbors of the node.
4. *Mean Square Error (MSE):* MSE is the difference between the estimated coordinate and the real coordinate of a sensor node. The trusted nodes are predicted accurately if MSE is minimum.

4.1. Average Residual Energy

The average residual energy of network for number of sensor nodes is shown in Figure 2. It is observed from the figure that the average residual energy of KM-TM is increasing when the number of sensor nodes is increased as compared to LDK+. The performance of KM-TM is enhanced 28% as compared with LDK+ for 50 nodes. This outperform due to that the key is shared in KM-TM between the trusted nodes only. Hence, energy consumption of the network is less in KM-TM as compared to LDK+.

Table 1. Simulation parameters

Parameters	value
Network area (m^2)	100 × 100
Number of sensor nodes (N)	100
Number of trust agents	10
Sink position	(50,50)
Initial Energy of the network	50 J
Packet size	512 Bytes

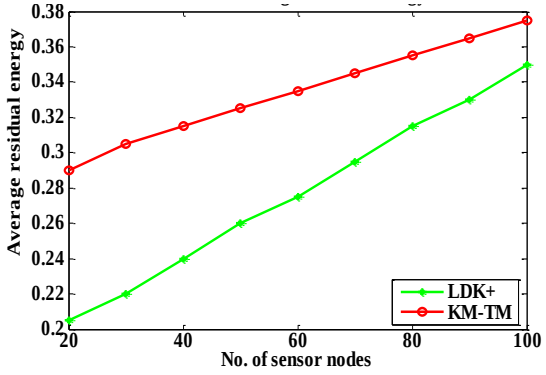

Figure 2. Average residual energy for number of sensor nodes

4.2. Total Node Death

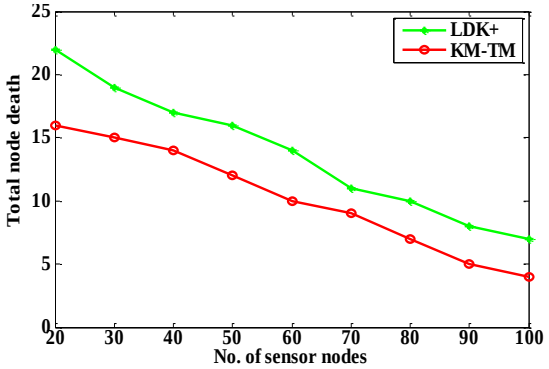

Figure 3. Total node death for number of sensor nodes

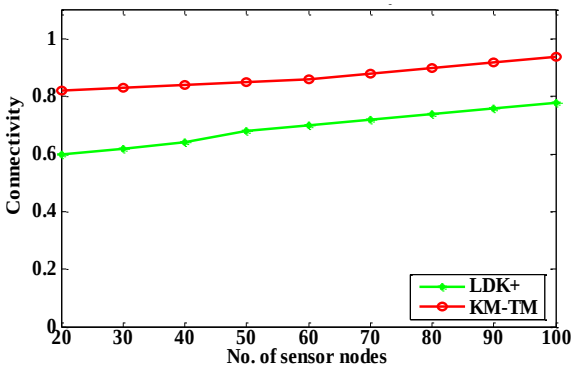

Figure 4. Connectivity for number of sensor nodes

The total death node is analyzed based on number of nodes used in the network. Figure 3 shows the death node versus sensor nodes used in a network. It is observed the performance of the KM-TM is better than that of LDK+. So, with the increase number of sensor nodes, the total node death rate decreases rapidly. The total node death rate of KM-TM is decreased by 36% for 50 nodes because the energy consumption is less in KM-TM compared to that of LDK+.

4.3. Connectivity

Figure 4 shows the connectivity between the sensor nodes. Note that connectivity analyzed based on the value between 0 and 1, when node has 1 indicates the complete connectivity amongst every node and its neighbors. Since, the key distribution takes place in the trusted path, the connectivity is increased by 18% for 50 nodes in KM-TM as compared to LDK+.

4.4. Mean Square Error

The MSE obtained for number of sensor nodes is shown in Figure 5. As the number of sensor nodes increases, the MSE increases rapidly. In 100 nodes scenario on an average it is clear that the MSE reduces by 27% for 50 nodes in case of KM-TM as compared to LDK+. In this way the trusted nodes are predicted with minimum error.

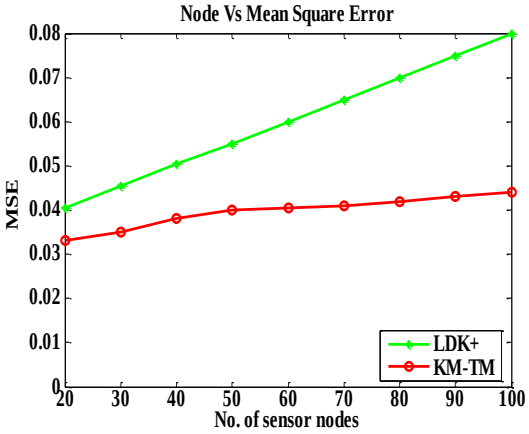

Figure 5. Mean square error for number of sensor nodes

5. Conclusion

The trust model has become important in many applications such as key exchange in a trusted manner, secure routing, and data gathering in a secure manner to detect threads in WSNs. Because of the wireless nature of WSNs, it requires a trust model in which sensor nodes are randomly deployed using neural networks where the trust agents monitor the sensor nodes. An efficient key management using trust model (KM-TM) for WSNs is proposed and its performance was evaluated in terms of residual energy, total node death, connectivity and mean square error. The residual energy of KM-TM is enhanced 28% for 50 nodes, the total node death rate of KM-TM is decreased by 36% for 50 nodes and the key distribution takes place in the trusted path, the connectivity is increased by 18% for 50 nodes in KM-TM as compared to LDK+. Simulation results show that KM-TM is an energy-efficient and attack-resistant trust based key management as compared to LDK+.

References

[1] IF Akyildiz, W Su, Y Sankarasubramaniam, E Cayirci. Wireless sensor networks: a survey. *Journal on Computer Networks.* 2002; 38: 393-422.
[2] Madhumita Panda. Security in Wireless Sensor Networks using Cryptographic Techniques. *American Journal of Engineering Research (AJER)*. 2014; 3(1): 50-56.

[3] Al-Sakib Khan Pathan, Hyung-Woo Lee, Choong Seon Hong. *Security in Wireless Sensor Networks: Issues and Challenges.* Proceedings of International conference on Advanced Communications Technology. Korea. 2006: 1043-1048.
[4] G Padmavathi, D Shanmugapriya. A Survey of Attacks, Security Mechanisms and Challenges in Wireless Sensor Networks. *International Journal of Computer Science and Information Security*. 2009; 4(1-2): 25-31.
[5] David Boyle, Thomas Newe. Securing Wireless Sensor Networks: Security Architectures. *Journal of Networks*. 2008; 3(1): 65-77.
[6] Khawla Naji Shnaikat, Ayman Ahmed AlQudah. Key Management Techniques in Wireless Sensor Networks. *International Journal of Network Security and Its Applications*. 2014; 6(1): 49-63.
[7] Swapna B Sasi, Dila Dixon, Jesmy Wilson. A General Comparison of Symmetric and Asymmetric Cryptosystems for WSNs and an Overview of Location Based Encryption Technique for Improving Security. *International organization of Scientific Research Journal of Engineering.* 2014; 4(3): 1-4.
[8] Enjian Bai, Xueqin Jiang. A Dynamic Key Management Scheme Based on Secret Sharing for Hierarchical Wireless Sensor Networks. 2013; 11(3): 1514-1523.
[9] Ali Hassan Sodhro, Ye Li, Madad Ali Shah. Novel Key Storage and Management Solution for the Security of Wireless Sensor Networks. 2013; 11(6): 3383-3390.
[10] W Jia, H Zhu, Z Cao, X Dong, C Xiao. Human-factor-aware privacy-preserving aggregation in smart grid. *IEEE Systems Journal*. 2014; 8(2): 598-607.
[11] T Kwon, J Hong. Secure and efficient broadcast authentication in wireless sensor networks. *IEEE Transactions on Wireless Communications*. 2010; 59(8): 1120-1133.
[12] LD Xu, W He, S Li. Internet of things in industries: A survey. *IEEE Transactions on Industrial Informatics*. 2014; 10(4): 2233-2243.
[13] C Fan, S Huang, Y Lai. Privacy enhanced data aggregation scheme against internal attackers in smart grid. *IEEE Transactions on Industrial Informatics*. 2014; 10(1): 666-675.
[14] L Eschenauer, VD Gligor. *A key-management scheme for distributed sensor networks*. In Proceedings of 9th ACM Conference on Computer and Commununications Security. Washington. 2002: 41-47.
[15] F Anjum. Location dependent key management in sensor networks without using deployment knowledge. *Wireless Network*. 2010; 16(6): 1587-1600.
[16] Jaewoo Choi, Jihyun Bang, LeeHyung Kim, Mirim Ahn, Taekyoung Kwon. Location-Based Key Management Strong Against Insider Threats in Wireless Sensor Networks. *IEEE Systems Journal.* 2015; PP(99): 1-9.
[17] Jinfang Jiang, Guangjie Han, Feng Wang, Lei Shu, Mohsen Guizani. An efficient distributed trust model for wireless sensor networks. *IEEE Transactions on Parallel Distributed Systems*. 2015; 26(5): 1228-1237.
[18] W Gao, G Zhang, W Chen, Y Li. *A trust model based on subjective logic*. In Proceedings of 4th International Conference on Internet Computer Science and Engineering. Australia. 2009: 272-276.
[19] M Chen, Y Zhou, L Tang. Ray projection method and its applications based on Grey Prediction. *Chinese J. Statist. Decision*. 2007; 1: 13-19.
[20] HS Lim, YS Moon, E Bertino. *Provenance based trustworthiness assessment in sensor networks*. In Proceedings of 7th International Workshop on Data Management of Sensor Network. New York. 2010: 2–7.
[21] E Elnahrawy, B Nath. *Cleaning and querying noisy sensors*. In Proceedings of 2nd ACM International Conference on Wireless Sensor Networks Applications. New York. 2003: 78–87.
[22] M Rabbat, R Nowak. *Distributed optimization in sensor network*. In Proceedings of 3rd International Symposium on Information Processing in Sensor Networks. New York. 2004: 20-27.