Security Using Dynamic Secret Based on Packet Loss Rate for Wireless Sensor Networks

Jingwen Yu[2], Jiechen Li[2], Zhanwei Xuan[2], Lei Wang[1,2] and Xiang Feng[1,2*]
[1]*College of Computer Engineering & Applied Mathematics, Changsha University, Changsha 410001, China*
[2]*Key Laboratory of Hunan Province for Internet of Things and Information Security, Xiangtan University, Xiangtan 411105, China*

Keywords: multi-hop networks, end-to-end transmission, data packet loss, dynamic secret

Abstract: The transmission security of wireless sensor networks plays a vital role in the application of the wireless sensor network. In order to protect these networks, many security protocols are proposed at this stage to protect the security of routing and data transmission. While much of the previous transport mechanism depends on the link layer encryption whose algorithms are not applied to end-to-end transmission. Thus there is scope for further research on the security of source node to sink transmission, and a new method that sink updates the key of the current group by calculating the packet loss rate and considering the local retransmission of the link layer is proposed. Our method provides a supplemental mechanism for existing transport protocols that even if an attacker eavesdrops the current key, the security is automatically replenished, thereby enhancing the security of the transmission. Theoretical analysis and simulation experiments show that the proposed method can guarantee the end-to-end transmission security, and it also consumes less energy than the application of dynamic key update directly to end-to-end transmission.

1 INTRODUCTION

A wireless sensor network (WSN) is composed of a large number of sensor nodes, which are powered by batteries and consist of data collection processing, sensing and short-range wireless communicating components (Akyildiz, 2002). It has a wide range of applications such as environmental monitoring, medical care, military field and target tracking (Yick, 2008). In a wireless sensor network, the source node communicates with the base station through multiple hops nodes, which only act as the forwarding nodes. Therefore, a node in a wireless multi-hop network not only can act as a source node to collect data but also can be an intermediate to forward data packets from other nodes. Since the sensors operate in an unattended, harsh or hostile environment and the lack of physical protection make the wireless sensor network vulnerable to attack or even physical damage, it is very important to ensure the communicating security of wireless sensor network (Kavitha, 2010).

Wireless sensor network is deployed with a large number of sensor nodes for data acquisition and processing capacity. However, the network is vulnerable to internal and external attacks because of the lack of tamper-resistant and the insecurity of a wireless communication channel. An attacker could capture, eavesdrop, and modify the information contained in the sensor node, even if injecting new information. Thus, there must be some kind of mechanism to deal with data transmission between nodes (Singh, 2011).

The purpose of security services in WSNs is to protect the information and resources from attacks. At present, many methods based on cryptography have been put forward to protect the security of WSNs and it is significant to choose the appropriate encrypted algorithm. A large number of researchers utilize the public key encryption to protect the wireless sensor network security (Gaubatz, 2004), (Watro, 2004), (Wang, 2006). However, the public key is characterized by high computational complexity, slow generation and high energy consumption. These methods are not suitable for a WSN with low power, low energy and weak computing power. Considering the above limitation of using public key encryption in wireless sensor, some improved methods based on the public key algorithm were also proposed for protecting the

Yu, J., Li, J., Xuan, Z., Wang, L. and Feng, X.
Security Using Dynamic Secret Based on Packet Loss Rate for Wireless Sensor Networks.
DOI: 10.5220/0008097001780183
In *Proceedings of the International Conference on Advances in Computer Technology, Information Science and Communications (CTISC 2019)*, pages 178-183
ISBN: 978-989-758-357-5

security of WSNs (Wander, 2005), (Gaubatz, 2005). Since the limitation on computational capacity and power consumption of the sensor nodes in a WSN, many methods based on symmetric keys were took into account to protect the security of WSNs (Liu, 2005), (Wang, 2008). For a WSN of N nodes in the Pairwise mechanism, each node needs to establish N-1 unique keys with all the other nodes in the network and maintain those keys in their memory in advance (Xiao, 2007). In addition, the sensor nodes are resource-constrained and the huge overhead also limits the applications of the above methods. Even if these keys can be successfully set up in WSNs and many studies have also demonstrated the safety of communication between two nodes through the encryption, it is difficult to guarantee the security of a WSN if the key once cracked by the attacker. Wireless communication contains a lot of potential vulnerabilities and is usually mobile, and an attacker can exploit these vulnerabilities to steal a key. It is difficult to construct a flawless security mechanism that can hold a secret forever, and a wireless user can not realize that the key has been stolen. When it is possible to steal the key, periodically update the key do not help much. No matter whether the key exchange uses symmetric or asymmetric encryption, once the key is stolen, the subsequently key exchanges become meaningless. Based on above problems, the literature (Xiao, 2007), (Xiao, 2010) proposed a method of updating the key dynamically to protect the security of WSNs. This method not only has the advantages of low computational complexity but also solve many of the limitations of wireless security. However, it mainly deals with communication problems between two nodes which dynamic secrets cannot be directly applied in multi-hop network. Because the dynamic secret is updated in real time based on the packets that the sink has not retransmitted, the data is forwarded from the source node through multiple nodes to the sink (the forwarding process does not update the key). If every two nodes update the key all based on the retransmission of the packet, this is bound to consume time and increase the computational complexity. Furthermore, each node is likely to be a source node and send data to the base station, thus it is also not suitable for using in multi-hop networks directly.

This paper presents a dynamic secret update mechanism based on packet loss rate to ensure the security of multi-hop network transmission. This paper is different from previous research where it no longer uses the physical layer channel model to construct a perfect key for encryption, and turn our attention to the link layer and transport layer. The point is to combine the dynamic secret updates with the existing security mechanisms. When a source node communicates with the base station, it is possible to determine whether the key is attacked based on the packet loss rate. If the key is attacked, the ongoing communication can generate a new dynamic secret to gradually restore security. We construct the secure mechanism which need to constantly update the system secret based on the transmission.

2 SCHEME OVERVIEW

Inspired by existing model based on dynamic secret to protect security transmission of data frames in the link layer(Xiao, 2010), we applied it to the end-to-end data transmission in the wireless sensor network. Sink counts the data packets received successfully from source node within time t and calculates the current packet loss rate p, then determines whether a new secret key is generated by comparing the current packet loss rate with the set threshold p_{th} so as to improve the security of the packet transmission between the source node and sink.

The data collected by the sensor node is divided into several groups, then each group is encrypted independently and forwarded to the sink which can decrypt and encrypt the packets according to the corresponding secret key. Furthermore, data is not encrypted or decrypted during the forwarding process of multiple hops. A secret key, which is the pairwise secret, is shared between the source node and sink to keep the communication security.

2.1 Notations and Symbols

Each node in the network shares a secret key with the base station. Apart from that, every packet collected by sensor node has a packet id of itself.

The following notations are used to simplify explanation in this paper:

i: The serial number of the packet collected by the source node (from $1 \cdots th$ where th is the threshold value that a node can store the maximum number of packets).

n: The number of packets in a group after grouped by a source node.

g: The category of each group of packets after grouping by a source node.

j: The new serial number of packets in each group is renumbered from 1 after grouping by a

source node (Where $j \leq n$).

p: Sink calculates the packet loss rate at time t.

k_c: The key for the c_{th} update, the initial key is k_0.

s_{c+1}: The dynamic key is generated after the c_{th} update.

φ_r: A collection of packets received by sink correctly (receiver)

φ_s: The source node (sender) receives a set of acknowledgment information within the specified time t.

3 ALOGORITHM PHASES

3.1 Calculating the Packet Loss Rate

The structure of the loss process in a sensor network is typically characterized by the packet loss rate. In general, the end-to-end packet loss rate is the percentage of the total number of packets that have not been successfully received by sink for a period of time and the total number of packets sent by the source node. Literature (Olsén, 2003) proposed a method of calculating the packet loss rate, which is calculated as follows:

$$p = \frac{N_{td}+N_{t0}}{N_s} \quad (1)$$

Where N_{td} denotes no of $TCP\ tripleduplications$ that the number of ACK packets that are repeated three times, N_{t0} denotes $no\ of\ TCP\ timeouts$ that the number of timeout packets and N_s represent $total\ no\ of\ sent\ packets$ that the total number of packets sent by the source node.

End-to-end transmission in a WSNs means that packets are transmitted from the source node to sink. If the packets have not successfully received by sink within time t, the retransmission request should be sent along the sink to the source node's reverse enhancement path. The required packet will be retransmitted when the retransmission request arrives at the source node. However, the end-to-end transmission process is usually accompanied by local retransmission of the link layer, since once a node has found a packet missing, it will send the retransmission request directly to the previous hop node.

3.1.1 Local Retransmission

In the intermediate node forwarding process is usually accompanied by local retransmission of the link layer, each intermediate node has the space to cache the current packet. As illustrated in the following Figure 1, supposing a source node transmits a set of ordered packets $m_1, m_2, \cdots, m_i, m_{th}$, then, once a node has found a packet missing at time t', it will send the retransmission request directly to the previous hop node. According to the following steps:

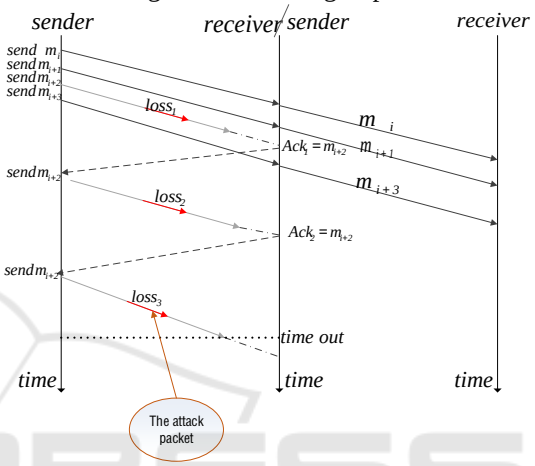

Figure 1: Local retransmission of the link layer.

Step1: The source node finds its neighbor node by the base station and divides the packet into the corresponding copies according to the number of neighbor nodes.

Step2: Writing the corresponding group for each packet, and the serial number of each group's packet is renumbered from 1.

Step3: For the sake of convenience in writing, the performance of packet developed into $[m_i]_{g|n}$, where "|" denotes connective symbol and "[]" indicate the same group of packets. In the transmission process, the neighbor node will detect whether the packet has been lost.

When the intermediate forwarding nodes discovers that the packet is lost, it sends a retransmission request to the previous hop node. If the packet is received by one or two retransmissions, it is not considered to be packet loss. If the packet is received by more than two retransmissions, it is considered to be packet loss and the node no longer sends the retransmission request.

3.1.2 End-To-End Retransmission

End-to-end transmission in a wireless sensor network means that the packet is transmitted from the source node to the sink, then sink sends the data

packet that needs to be retransmitted with the next set of packets, renumbering it and sending it to the neighbor node. Sink counts this type of packet loss and calculate the packet loss rate after a source node transmits a set of data. Comparing this packet loss rate with the set threshold, if the packet loss rate is greater than the set threshold, indicating that the transmission of security risks and need to do a series of measures to restore its security; if the packet loss rate is less than the set threshold, indicating that the transmission is relatively safe and the current key is reliable.

3.2 Dynamic Secret Key Generation

3.2.1 Determine Whether the Key Needs to be Updated

Sink calculates the packet loss rate for this group after a source node transmits a set of data and compares this packet loss rate p_j with the set threshold p. Where j represents the j_{th} group of packets sent by the source node to the sink node.

- $p_j > p$ indicating that the transmission of security risks and need to update current key.
- $p_j \leq p$ noting that the transmission of this group is reliable in the case of allowing a certain packet loss, so there is no need to update the current key.

Obviously, the number of updates which proposed in this paper is less than that of Xiao Sheng's proposal, thus reducing the amount of computation and energy consumption accordingly.

3.2.2 Affiliations

Assuming that the initial key is k_0 and the current key is k_c (the c_{th} updated key), the key is updated to k_{c+1} if it satisfied with the update condition and the key generation process is as follows:

$$k_{c+1} = k_c \oplus s_{c+1} \quad (2)$$

$$k_{c+2} = k_{c+1} \oplus s_{c+2} = k_c \oplus s_{c+1} \oplus s_{c+2} \quad (3)$$

$$k_{c+n} = k_{c+n-1} \oplus k_{c+n} = k_c \oplus s_{c+1} \oplus s_{c+2} \oplus \cdots \oplus s_{c+n} = k_c \oplus \sum_{j=1}^{n} s_{i+j} \quad (4)$$

Where s_{c+1} is the generated dynamic secret, algorithm in the following sections will only operate on the synchronized φ_r and φ_s. Therefore, we unify the notion as $\varphi = \varphi_s = \varphi_r$, respectively, $\varphi_s = \varphi_r = \emptyset$ before communication begins.

The packets received by the receiver belong to φ_r that is $n|k|m_i \in \varphi_r$;The sender receives confirmation from the sink node within the prescribed time, then $n|k|m_i \in \varphi_s$.

(a): If the sink node calculates the packet loss rate ρ = 0, there is no packet loss during the end-to-end transmission and return the confirmation message $Ack = no\ loss\ of\ data\ packets$. Continue sending the next set of packets according to the local retransmission step after the sender receives the confirmation message within the specified time,

(b): If ρ> 0, there is a packet loss. Assuming that sink determine the information of the lost packet is $n|k|m_l$, then return confirmation information $Ack = n|k|m_l$ to source node. Sender within a specified time to receive confirmation information, then the packet to be retransmitted $n|k|m_l$ with the next set of data packets sent synchronously and repeat the local operation of the retransmission.

Definition 1: ∀ data packet $n|k|m_i$, $n|k|m_i \in \varphi_r$、$\varphi_s \Longrightarrow \varphi = \varphi_s = \varphi_r$

$$s_{c+i} = hash(\varphi) \quad (5)$$

It is very difficult for the adversary to reproduce φ. Not only must she eavesdrop every data packet, but also all of the acknowledgements and retransmissions of link layer. Otherwise, even if she can receive a data packet correctly, she cannot identify whether this packet is an φ or not. Whenever the adversary is uncertain about φ, the uncertainty is reflected in the dynamic secrets. Furthermore, sink knows the packet loss rate of the source node, and the intermediate node does not know the packet loss rate between the source node and sink. Above all, the packet loss rate is related to the need to update the key, so even if intermediate node has compromised, it cannot know how much packet loss between sink and source node, thus do not know whether the dynamic key in the transmission has updated or not. Therefore, our paper enhances the dynamic secret update uncertainly and improves transmission security.

4 SECURITY ANALYSIS

4.1 Secure End-To-End Transmission

In order to ensure the authenticity and confidentiality of packets that transmitted from

source node to the base station, we proposed a secure mechanism that dynamically update the secret based on packet loss rate. Each source node in the sensor network establishes an initial symmetric key with the base station. We can randomly transmit some packets to test whether the sensor network is secure before the source node sends data packet to the base station. If the sensor network is secure, the required data packets begin to be transmitted. The source node and sink will update the shared key between them only the packet loss rate is greater than the set threshold. An attacker would lose the unrecoverable information If he/she could not eavesdrop a transmitted packet at the beginning. This means that the attacker cannot steal the key, and the key is updated immediately if the transmission is found to be insecure.

There are two advantages to prevent the attacker to steal the key. On the one hand, the attacker does not know which node need to send data to the base station, and which node sent the eavesdropped packet. Furthermore, the attacker need to determine whether the transmitting packet is sent from the node or through the node. On the other hand, packets of the source node are distributed sent to the neighbor nodes. The attacker cannot steal all the packets sent from one source node at the same time so that cannot steal key by eavesdropping the packets.

4.2 Secure Point-To-Point Forwarding

The communication distance of the nodes in the a WSN is limited, so the data packets transmitted by the source node to the base station need to be forwarded through the intermediate nodes. The packet in the forwarding process cannot be encrypted by the intermediate node and the authenticity and confidentiality of these packets are mainly verified by the dynamic key between the source node and the base station.

Although the packets are not encrypted hop-by-hop in the forwarding process, it also can guarantee the transmission security because the packet will be verified the integrity between any two nodes. If the integrity of the packet is broken, the node will send a retransmission request; If the same packet need to be retransmitted more than twice between two nodes, it will be discarded. The base station will request the source node to retransmit the packets that were actively discarded during the forwarding process.

5 EXPERIMENT

All simulation is performed using MATLAB, and we make the following assumptions in order to facilitate the comparison of experiments:

I. All packets are delivered without error or loss,

II. The end-to-end of our paper is equivalent to the two nodes without considering the forwarding of the intermediate nodes.

III. The number of packets transmitted by the sender at the unit time is the same.

IV. The threshold for data packet update in the experiment is 20, and the threshold for our method is 0.1. Furthermore, the experiment was repeated 100 times.

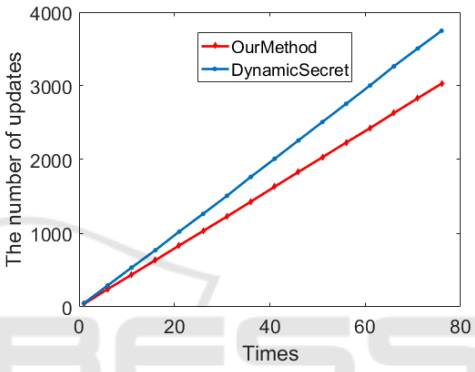

Figure 2: The number of updates.

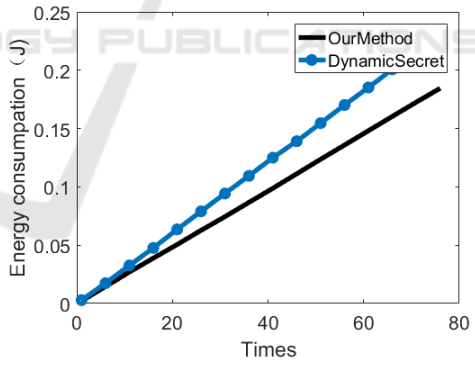

Figure 3: Energy consumption.

Figure 2 compares the numbers of update required to secure communication using our method or dynamic secret. The numbers of update represent the number of key updates after the arrival of the lifetime of the networks. Figure 2 shows that it need to be updated 392 times for our method and 493 times for dynamic secret at 10s. Our method requires 79 percent of the numbers of update needed by dynamic secret and as times goes by, the number of updates for his method grows faster than our approach, showing immediate gains in security overhead.

Figure 3 compares the energy consumption required to secure communications using our method or dynamic secret. Showing that it need to consume 0.09 joule of energy for our method and 0.122 joule energy for dynamic secret at 40s. Our method consumes 78 percent of energy by dynamic secret. Figure 3 shows that our method consumes less energy than dynamic secret in the case of security.

Our method demonstrated the effectiveness of its protocol, showing itself to be far more scalable than dynamic secret. A clear trend is shown, in which our method more slowly increases in the numbers of updates and energy consumption compared to dynamic secret.

6 CONCLUSIONS

A novel key update approach to enhance the security of a multi-hop wireless sensor networks, when eavesdropped by attacker. The primary focus is to update the key dynamically based on data packet loss rate that allows expedient, reliable communication with confidentiality, integrity and authenticity services. This model accounts for the end-to-end retransmission and the local retransmission of the link layer, which improves the security of data packets transmission in the multi-hop networks. Our solution is to generate a series of hash values from the communication process, and apply these hash values to constantly update the key. The adversary is uncertain about dynamic secret. Moreover, it does not know whether the dynamic key in the transmission has updated. As the transmission of data packets goes on, communication security keeping replenishing itself as if the wireless communication system has powerful function to resist attacks.

ACKNOWLEDGEMENTS

The authors thank the anonymous referees for suggestions that helped improve the paper substantially. The project is partly sponsored by the National Natural Science Foundation of China (No.61873221, No.61672447), the Natural Science Foundation of Hunan Province (No.2018JJ4058, No.2017JJ5036), Hunan province science and technology project funds (No.2018TP1036), and the CERNET Next Generation Internet Technology Innovation Project (No.NGII20160305, No.NGII20170109).

REFERENCES

Akyildiz I F., Su W., Sankarasubramaniam Y., et al., 2002 A survey on sensor networks[J]. *IEEE Communications magazine*.

Yick J., Mukherjee B., Ghosal D., 2008. Wireless sensor network survey[J]. *Computer networks*.

Kavitha T., Sridharan D., 2010. Security vulnerabilities in wireless sensor networks: A survey[J]. *Journal of information Assurance and Security*.

Singh S., Verma H K., 2011. Security for wireless sensor network[J]. *International Journal on Computer Science and Engineering*.

Gaubatz G., Kaps J P., Sunar B., 2004. Public Key Cryptography in Sensor Networks--Revisited[C] *ESAS*.

Watro R., Kong D., Cuti S., et al., 2004. TinyPK: securing sensor networks with public key technology[C] *Proceedings of the 2nd ACM workshop on Security of ad hoc and sensor networks. ACM*.

Wang Y., Attebury G., Ramamurthy B., 2006 A survey of security issues in wireless sensor networks[J].

Wander A S., Gura N., Eberle H., et al., 2005. Energy analysis of public-key cryptography for wireless sensor networks[C]*Pervasive Computing and Communications, 2005. PerCom 2005. Third IEEE International Conference on. IEEE*.

Gaubatz G., Kaps J P., Ozturk E, et al., 2005. State of the art in ultra-low power public key cryptography for wireless sensor networks[C]//*Pervasive Computing and Communications Workshops, 2005. PerCom 2005 Workshops. Third IEEE International Conference on. IEEE*.

Liu D., Ning P., Li R., 2005. Establishing pairwise keys in distributed sensor networks[J]. *ACM Transactions on Information and System Security (TISSEC)*.

Wang H., Sheng B., Tan C C., et al., 2008. Comparing symmetric-key and public-key based security schemes in sensor networks: A case study of user access control[C]//*Distributed Computing Systems, 2008. ICDCS'08. The 28th International Conference on. IEEE*.

Xiao Y., Rayi V K., 2007. Sun B, et al. A survey of key management schemes in wireless sensor networks[J]. *Computer communications*.

Xiao S., Gong W., 2010. Mobility can help: protect user identity with dynamic credential[C]//*Mobile Data Management (MDM), 2010 Eleventh International Conference on*.

Xiao S., Gong W., 2010. Towsley D. Secure wireless communication with dynamic secrets[C] *INFOCOM, 2010 Proceedings IEEE*.

Olsén J., 2003. On Packet Loss Rates used for TCP Network Modeling[J]. *Mathematical Statistics*.