Routing Strategy and Data Security Technology in IPv6 Wireless Sensor Networks

https://doi.org/10.3991/ijoe.v14i08.9181

Zhaoyan Li(✉), Chengfang Zhao
Xihua University, Chengdu, Sichuan, China
zhaoyanli1293@163.com

Abstract—A new routing rule detection and identity authentication mechanism based on the path sequence is proposed to cope with the vulnerability problem of wireless sensor networks (WSNs) against various attacks, especially in unattended environments. Then, the great permutation encryption algorithm (G-PEC) for WSN is proposed. Finally, a signature scheme against pollution attack based on linear network coding is improved. The results show that the proposed path sequence-based authentication method with the Contiki simulation platform can significantly reduce the computing overhead of sensor nodes and decrease the energy consumption and delay of nodes to a greater extent than the traditional authentication method. The G-PEC can effectively resist eavesdropping attack, and the new signature scheme does not need additional secure channels. The proposed mechanism also provides source message authentication.

Keywords—wireless sensor network, routing authentication, network coding, permutation encryption, homomorphic function

1 Introduction

Wireless sensor network (WSN), a new network form, is partly similar to traditional networks and partly distinctive in terms of characteristics. WSNs are more vulnerable than wired networks. A wired network is difficult to attack because of its physical isolation, whereas WSNs are easily affected by security threats, such as message injection, information tampering, and eavesdropping and interception. In addition, attackers of sensor networks do not need to be limited by the characteristics of sensor nodes because they may use expensive transceivers and main power supply nodes, which then renders this type of network to be easily affected by security breach.

The security issues of WSNs have been a popular research topic not only because of the commonality of their security threats (e.g., message injection, forgery, tampering, and so on), but also because the threats can deplete energy due to disk operating system attacks. A security breach can extensively limit the operations of many applications once the destructive attack reaches the WSN and destroys the constituent nodes. To ensure a secure working environment, a lightweight security mechanism needs to be designed that will enable the WSN to be applied to various fields. Certain characteristics, such limited storage resources, restricted computing communication capability, and so on, of WSNs must be considered in the design process.

In the studies on security based on WSNs, cryptographic mechanisms are often proposed to effectively resist attacks, such as message injection, eavesdropping, and tampering. End-to-end encryption mechanisms can specifically prevent message eavesdropping from captured intermediate nodes, but the encryption mechanism needs to establish a key between end nodes. However, this approach is not suitable for multicasting and broadcasting systems. Although link layer encryption is much simpler, or even if a shared key can be used to support multicasts and broadcasts, the intermediate nodes may still eavesdrop or tamper information. The security requirements of WSNs generally include the following: confidentiality, availability, integrity, authority, non-repudiation, and real-time characteristics.

In view of the vulnerability of WSNs to various network attacks, this paper discusses routing strategies and data security technologies. First, the security requirements of WSNs based on IPv6 are introduced. Then, the routing protocol (RPL) used in the implementation of security mechanism is briefly described. Finally, a signature scheme against pollution attack based on linear network coding is proposed. In summary, the great permutation encryption algorithm (G-PEC) can effectively resist eavesdropping attacks and provide source message authentication.

2 State of the art

The rapid development of wireless communication technology has extended the application of WSNs to agricultural and industrial fields, environmental protection, and military affairs. Some scholars have designed lightweight RPLs and security mechanisms based on the limited resource constraints of WSN. However, the receiving and sending ranges of wireless sensor nodes are extremely limited due to storage and energy restraints. Nonetheless, in actual deployment, the nodes can be formed with multi-hops to extend the environmental monitoring area and widen the range of the sensor network. The nodes can also be designed to transmit the perceived data to the sink node. Therefore, designing a secure RPL for WSNs that can both minimize the energy consumption of nodes and satisfy the transmission accuracy of packets is an urgent endeavor.

To solve the problem related to the maximization of throughput of multicast networks, Naranjo et al. (2017) proposed that low transmission delay, low energy consumption, strong robustness, and other performance measures be realized in all kinds of communication systems [1]. Li et al. (2016) proved that stochastic linear network coding can achieve optimal throughput in multicast networks, as opposed to random linear network coding, which is typically considered for its effective network coding paradigm and its network nodes that linearly use random coefficients to combine input data packets [2].

Knowing how to prevent eavesdropping attacks against encoded packets in WSN, especially during random network coding, is an urgent and challenging problem. To reduce the cost of throughput, Yuvaraja et al. (2017) designed a network coding with network security based on how attackers intercept limited numbers of packets [3].

Logambigai et al. (2016) obtained weak security after transforming source node messages, but they did not lose any system capacity [4].

Orojloo (2016) proposed a scheme in which a set of encoding vectors was encrypted by the source node, while the group of unencrypted encoding vectors retained the standard encoding process in the intermediate node. The scheme clearly needed to be encrypted with less data segments but required two rounds of decoding, and the two sets of encoding vectors had high space overhead [5].

Ferng et al. (2016) combined the problems of key management and low authentication efficiency in the existing security schemes in WSNs and proposed a lightweight security system suitable for those networks [6]. Guo et al. (2017) proposed a permutation encryption algorithm based on the network coding in p-coding, which not only effectively resisted eavesdropping attacks but also was lightweight and suitable for WSNs [7].

Rao et al. (2018) proposed the homomorphic hash scheme, while Charles and so on (2016) designed a new homomorphic signature scheme [8]. Zhu et al. (2016) proposed a new signature scheme based on the linear characteristic of network coding [9], in which the node can quickly verify the integrity of the packet. Gomez et al. (2017) proposed a new homomorphic signature scheme based on discrete logarithms [10] during the INFOCOM 2008, and its particular contribution centers on intermediate nodes that not only generate signatures for their output messages but also do not have effective signatures for contaminated or forged packets. The homomorphic signature scheme does not need to create additional security channels to transmit the hash table of messages. Whether the signature scheme is homomorphic or not can be verified in the future, but this current knowledge gap also implies that the scheme cannot be verified by homomorphism during message authentication, which further suggests that the validation efficiency will be low and not applicable to WSNs.

The established RPL and the designed encryption technology both focus on security, but the latter can utilize the corresponding security RPLs against each particular attack. Zhu et al. (2017) proposed a symmetric key management technology and built a unique symmetric key between each node and trusted sink node for identification [11].

Thang et al. (2015) proposed a stateless RPL general packet service radio with broadcast detection [12] to which time delay judgment was added on the basis of the routing mechanism. The RPL system was highly reliable, but the contribution of RPLs on energy consumption was not specified.

In summary, the abovementioned security mechanisms are mainly based on the limited eavesdropping ability of opponents. However, smart opponents can sufficiently intercept packets and defeat different security mechanisms by monitoring other network links and collaborating with other malicious nodes. The encryption mechanisms of WSN coding therefore needs to be investigated to prevent the occurrence of more powerful attacks. On the basis of the status of existing research, the present study proposes a global encoding vector permutation encryption algorithm that is more lightweight than the previous scheme on the premise that the same security target can be reached. The homomorphic signature scheme is also improved. In the scheme, the source node uses a private key to sign the message, while the other nodes use the public key of the source node to detect the received message.

3 Path sequence routing detection and authentication in WSN

3.1 Path sequence WSN secure routing detection mechanism

The implementation process of path sequence routing detection (PSRD) can be divided into three stages: routing establishment, path sequence generation, and data security processing. The specific process is shown in Figure 1.

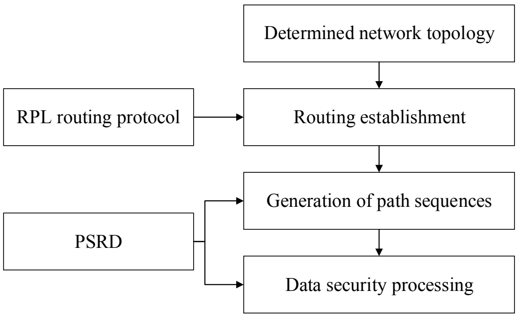

Fig. 1. PSRD flowchart

First, the RPL adopted in this scheme searches the optimal path to the sink node according to the minimum hop count. In the initialization stage where the routing is established, the sequence of all paths of the entire network is generated and the path sequence of the node is stored on each node. Then, in the message data transmission stage, each node implements routing rule detection and identity authentication by verifying the path sequence forwarded to the received packet to ensure the correctness of the routing rules and the authenticity of the data.

After establishing a good route according to the RPL in the WSN, a path sequence needs to be generated and the entire network needs to be informed about this configuration prior environment data transmission to ensure that the initialized routing table (RT) is well stored on each sensor. For a WSN with a network cluster size of N nodes,

$$T_i = t_{k-1}t_{k-2}...t_1t_0 \in \{0,1\}^k (i = 1,2,...,d; d = 3,4...). \tag{1}$$

The d table item (T1, T2, T3,..., Td) ∈ RT of the routing information table on a specific sensor node represents the path sequences of bar routing through the node, which then are used for the routing rule detection and identity authentication of packets that pass through the node in the subsequent data transmission process.

The length of the path sequence needs to be rationally designed to reduce the probability of attack detection failure. The length of the path sequence is designed to be b bytes while the number of nodes in the WSN cluster is n. When the network scale is continuously increased, the parameter decreases 1/2 k faster than that of the RT table item d number under the same node. Subsequently, the probability of $1-(1-1/2^k)^d$

tends to be low. The application security of this mechanism is higher when the network is larger.

To understand the specific impact of network size on PSRD security, the relationship between the probability of detection failure and the number of RT items of any intermediate node based on the probability model of attack detection failure is explored.

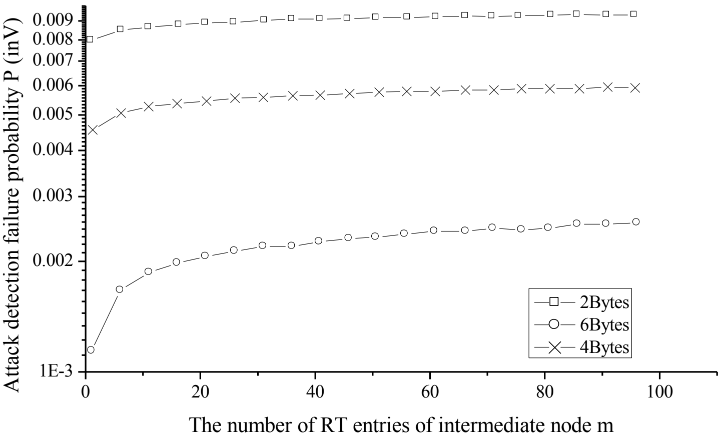

Fig. 2. Relationship between the probability of PSRD attack detection failure and the number of node RT table entries

The length of the path sequence is 2, 4, and 6 bytes, which correspond to WSNs with network scales of 2^8, 2^{16}, and 2^{24}, respectively. Therefore, the network scalability of the security mechanism is good. As shown in Figure 2, for networks with fixed sizes, the greater the number of RT entries is after a node, the lower the security will be. In addition, when the size of the network increases, the bit length of the path sequence also increases correspondingly, and the value of $1-(1-1/2^k)^d$ will decrease theoretically. Thus, relative to the three curves in Figure 2, the probability of failure when the mechanism conducts attack detection will be significantly reduced for WSNs with relatively long network path sequences.

3.2 General applicability of attack models

WSNs encounter various kinds of network threats. Regardless of the type of threat, WSNs are expected to analyze the security and effectiveness of their PSRD mechanisms.

Message injection attack is an active attack that forwards false messages to a network. The typical aim of the attacker is to pollute network data or render the network saturated by transmitting false messages. Owing to their specific characteristics, the WSNs become vulnerable to message injection attacks. For example, in terms of the application of WSN in fire warning, false news can generate wrong warning signals and waste manpower and material resources.

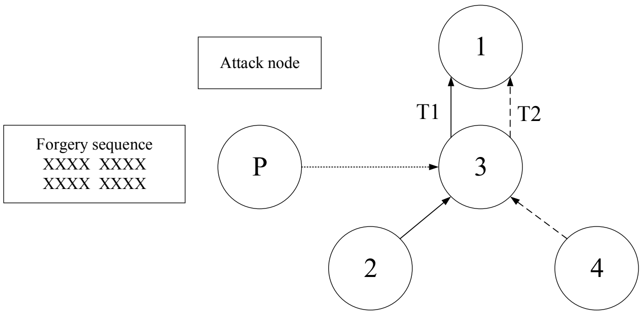

Fig. 3. Sample diagram of message injection attack

Figure 3 presents T1 and T2 as two established routing path sequences. All nodes that pass through the two paths are known, but the subsequent inclusion of illegal nodes are unknown. This study assumes that message injection attack node P, which later connects with the network, randomly forges a sequence of T_p and forwards it to the pollution packet, which is sent by the attack itself. The probability of the attack detection failure is $3.05*10^{-5}$ based on the verified path sequence in the subsequent legitimate forwarding node. When the pollution packet from node P reaches node 3, this node can detect the message injection attacks with 99.997% probability and promptly discard the illegal packets.

3.3 Analysis of system simulation performance

Given their different computational complexities, the time requirements of the WSN nodes to handle packet security by using PSRD or cerebellar model articulation controller (CMAC) also vary. The security processing time delays of the two algorithms are evaluated for their performance index. The implementation time of each security processing algorithm for each node is generated and measured with the Mote Output of the Cooja simulator.

In the PSRD and CMAC algorithms, the statistical average of implementation time of each fixed length message is measured and the length of the message is changed for multiple measurements. When the size of the network increases, the byte length of the path sequence also increases, which then leads to a slight increase in the implementation time of PSRD during the verification of long sequences, but this effect is extremely small and negligible. To simplify the measurement, the length of the sequence is set to 2 bytes.

Table 1. Node processing delay of PSRD and CMAC with different length data

Data length (byte)	20	40	60	80
PSRD time (ms)	0.22	0.36	0.27	0.32
CMAC time (ms)	4.2	5.6	7.1	8.5

If the node recorded in Table 1 has a single-time delay statistical mean for single-security processing, then the processing delay of PSRD is nearly 0. By contrast, the time of implementation of the CMAC algorithm is much larger. The difference can be attributed to CMAC that requires [|M|/128]+1 AES packet encryption operation during the processing of message with lengths of |M| bits. By contrast, PSRD only needs to retrieve and match the path sequence in its own RT, and it does not need to run any encryption algorithm. When the message length is increased, the number of advanced encryption standard (AES) encryption in CMAC also increases, which result in the continuous rise in security processing delay. By contrast, PSRD is only involved in the processing of path sequences forwarded to packets; it does not handle message text content, and thus, its implementation time is irrelevant to message data length. The experimental results are consistent with the theoretical analysis.

The implementation time of data security processing reflects the performance of an algorithm to efficiently forward or receive data. The more efficient the algorithm is, the less time it takes to process data; moreover, the shorter the delay is, the better the algorithm performance will be. These correlations depict a highly important aspect of the performance index, especially for WSNs with large amounts of sending or forwarding environmental data or high real-time requirements. The results show that the proposed PSRD is superior to the traditional authentication algorithm (i.e., CMAC) in terms of node security processing delay performance.

Due to the differences in their computational complexity, the energy consumption characteristics of the central processing units (CPU) of the WSN nodes of PSRD and CMAC also vary. The greater the amount of computation is, the greater the energy consumption of the node CPU will be. The nodes are powered by batteries that cannot be promptly replenished once the energy is exhausted. The premature exit of one or some nodes in the network may cause the local failure of sensor networks. Considering that the energy of the sensor nodes is severely limited, a good authentication algorithm with the smallest energy loss possible is needed to ensure network security. Consequently, the lifetime of the node can be maintained in the long term.

The total energy consumption on the sensor nodes consists of the energy-consuming CPU and the library of parameterized modules (LPMs), among others. Given that only the CPU will run in the sensor nodes when the algorithm operation is performed, the activity time of the LPM is 0 whereas the CPU consumes energy at this time. The software-based energy consumption measurement mechanism (Energest) of the Contiki operating system is used to derive the single-running time of each module of the nodes during authentication and detection. The formula of energy consumption (i.e., CPU) is

$$E(J) = \left(cpu_{endtime} - cpu_{starttime}\right) \cdot 1.8mA \cdot \frac{3V}{4096} / 1000 . \tag{2}$$

The statistical mean values of the energy consumption of the CPU for each fixed length message are measured with the PSRD and CMAC algorithms by using Energest. The lengths of the messages are changed for multiple measurements. When the size of the network increases, the length of the path sequence will also increase, which then leads to a slight increase in the energy consumption of the PSRD during the validation of long-sequenced CPU. However, this effect is extremely small and negligible. To simplify the measurement, the length of the sequence is set to 2 bytes.

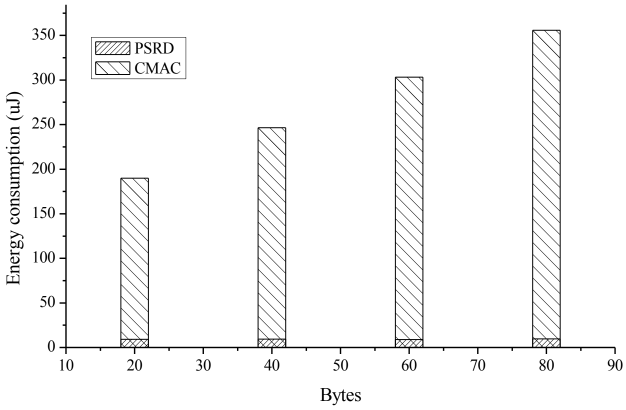

Fig. 4. CPU energy consumption of PSRD and CMAC under different length data

Figure 4 presents the statistical average of the energy consumption of the CPU for the single-security processing of nodes by using the two algorithms. The result shows that the PSRD authentication method is superior to the traditional authentication algorithm (i.e., CMAC) in terms of energy consumption performance. When the message length is increased, the number of AES encryption in CMAC also increases, which renders a higher energy consumption for the CPU. By contrast, PSRD only processes the path sequence forwarded to the packet, and it does not handle message text content. Thus, the CPU energy consumption caused by the implementation of PSRD is not related to the length of message data.

For WSNs that are generally deployed in unattended harsh environments, the energy of the sensor node battery is severely limited. The main advantage of the authentication mechanism based on the path sequence is that it does not involve encryption algorithm operations that consume large amounts of computing resources, and thus, the amount of computation is minimal. The WSN that uses this security mechanism can save a certain amount of CPU energy consumption during the authentication and detection calculation of each sensor node. Therefore, the network lifetime of WSNs in constant operation can be remarkably extended.

4 Global coding vector replacement encryption based on network coding

Eavesdropping is a common security threat in WSNs, and the common anti-interception model is message encryption. However, traditional end-to-end full text encryption methods, such as block cipher algorithm RC5 and RC4 and the tiny encryption algorithm, are not applicable due to limited node resources. Some cryptographic technologies, such as data encryption with high computing power, are also not applicable to WSNs. Based on the abovementioned considerations, a lightweight network security technology will be the future research direction of WSNs. At present, the research on this topic is divided into three aspects: lightweight encryption algorithm, lightweight routing mechanism, and lightweight authentication mechanism.

As opposed to the traditional end-to-end full text encryption, G-PEC encrypts the global encoding vector only once. Figure 5 presents a comparison of the traditional encryption algorithm and G-PEC that requires encrypted message lengths. The ZigBee packet is used, and the standard packet length is 128 bytes. Given that the traditional encryption method is based on end-to-end full text encryption, the length of the encrypted packet accords with the length of the original text. The G-PEC algorithm encrypts the global coding vector part only. Subsequently, the length of the encrypted data is considerably reduced, which suggests reduced complexity of data encryption.

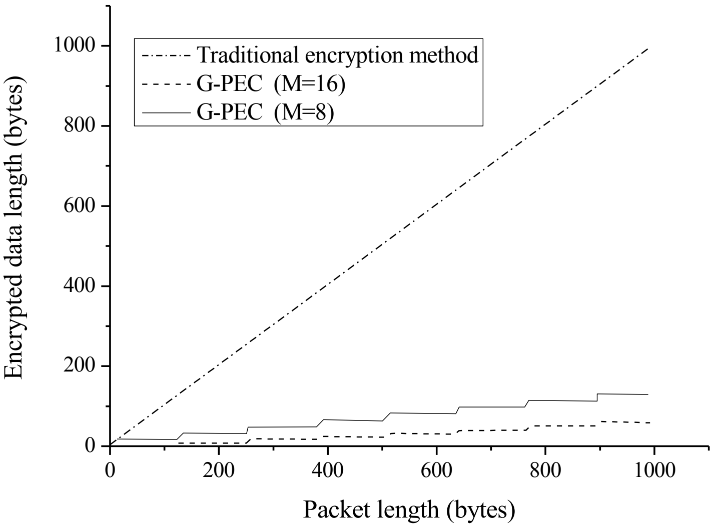

Fig. 5. Comparison of G-PEC and traditional encryption complexity

Figure 5 compares the encryption algorithm complexity of the G-PEC and traditional encryption algorithms at m = 8 and m = 16. The length of the message packets for G-PEC encryption is the staircase type because the sub-package is utilized when the message length exceeds that of the ZigBee packet standard, and a new message packet is generated. Moreover, each packet contains global encoding vectors that need to be replaced by encryption.

We assume that the source node and the sink node are secure and will not be attacked by eavesdroppers. The previous analysis shows that useful information is difficult to obtain even if an attacker has sufficiently tapped and intercepted the packets. The subsequent paragraphs present our analysis from a theoretical viewpoint.

Assuming that the message packets sent by the source node are sent in their totality and all lengths are equal. Using G-PEC does not affect the length of the original message. According to its algorithm mechanism, the encoded message length is n = a+m+L. The key of the replacement encryption is randomly generated. Thus, if an eavesdropper intends to decrypt data packets, then the same key must be derived. The probability satisfies the following equation:

$$P\left(\bigcap_{i=1}^{n}\left\{C(i)=x_{h(i)}\right\}M=x\right)=\frac{1}{A_n^m},(\forall h,\forall x). \tag{3}$$

The number of regions required to generate the same random key as the original replacement encryption key is A_n^m. We also assume that the number of messages to be obtained by attackers is higher than m, brute force is used for cracking, and the complexity of the message before the permutated encryption can be obtained as $O\left(A_n^m\right)$. The Gauss elimination method is also performed to obtain the original packets, in which the complexity of the Gauss elimination is $O\left(m^3\right)$. The complexity of brute force cracking remains to be $O\left(A_n^m \cdot m^3\right)$ even if packets can be sufficiently intercepted. If the computing power of the eavesdropper is 10 instructions per second, then the time spent by the eavesdropper to derive the original message is

$$T=\frac{A_{128}^{16}\times 16^3}{365\times 24\times 3600\times 10^{20}}=2.5366\times 10^9(year). \tag{4}$$

The analysis shows that even if the eavesdropper can sufficiently intercept the packets, it is unable to use brute force to obtain any useful information. The G-PEC algorithm effectively reduces the complexity of the encryption and improves the ability of the system to resist eavesdropping threats.

5 Anti-pollution attack homomorphic digital signature based on network coding

5.1 Homomorphic signature scheme for anti-pollution attack

The proposed scheme enables intermediate nodes to promptly and effectively detect and dispose contaminated messages, thus achieving high efficiency even when computing resources are limited. In addition, the scheme does not require additional security channels.

The framework of the digital signature scheme used to solve the pollution attacks during linear network coding is divided into three stages. (1) Parameter setting: In this stage, the source nodes select security parameters, private and public keys, and digital signature functions. (2) Digital signature calculation: The source node calculates the digital signature value for its message. The signature values will be transferred to intermediate nodes and sink nodes. (3) Message validation: The intermediate node and the aggregation node verify the received message, which is based on the encoding vector embedded in the message, the digital signature of the message, and the public key of the source node. If validation is successful, then the received messages will be accepted for further encoding or decoding; otherwise, they will be discarded.

5.2 Performance analysis

In network coding, the middle node needs to verify the integrity of a message. Thus, the main factor that affects the message's fast or slow transmission in the network is the speed of the intermediate node to verify the message. The network performs better when the speed of message verification is faster; otherwise, the entire network will experience a bottleneck, which prevents the source node from sending messages at optimum speed.

In the proposed algorithm, apart from the m+n order power operation of the hash value of the message, the node needs to perform a modular exponentiation of the RSA signature. Assuming that the time complexity of each model power calculation is O(1), then the total time complexity is O(m+n+1). The time complexities of the comparator algorithms are O(m+n), in which the hash value of the node for the received message corresponds to power operation by m times, while that of the source message corresponds to power operation by n times. Compared with other operations, such as addition or subtraction modules, the modular exponentiation dominates the message verification stage. Therefore, the cost ratio of our scheme on message verification is (1+m+n) / (m+n) ≅ 1. In the algorithm, the verification requires m+n exponentiation each time; thus, the time complexity is O(m+n).

Table 2. Time complexity of three algorithms (in modular exponentiation).

Algorithms	This algorithm	GR	ZKM
Time complexity	O(m+n+1)	O(m+n)	O(m+n)
Does it need additional security information channel?	No	Yes	Yes

According to Table 2, this algorithm performs well in terms of verification efficiency, mainly because it does not require additional security information channels, relative to the two other algorithms. In addition, because this scheme is based on the digital signature function, it can authenticate source messages.

One of the purposes of using network coding in WSNs is to reduce resource wastage. Therefore, the load overhead of node messages in the network is another important parameter when assessing the quality of algorithms. Each message data, including the coefficient vector, is a vector with m+n dimension. The length of each scalar is $\log(u)$ bit, and the length of the message is $(m+n)\cdot\log(u)$ bit. The public key with a length of $m\cdot\log(u)$ is transmitted with the message. The load overhead of each message generation is $m/2m+n$.

6 Conclusion

The security of WSNs is explored in this paper. First, the security requirements of WSNs based on IPv6 are introduced. Then, the RPL used in the implementation of security mechanism is briefly described. The common network attacks and the security mechanisms of the WSNs are investigated for subsequent design and improvement. Finally, simulation verification and performance analysis are performed. The software-based performance evaluation results show that PSRD can better reduce the node security processing delay and the energy consumption of CPU compared with the traditional authentication algorithm (i.e., CMAC). Under the condition of lower encryption complexity and computational cost, G-PEC has higher security performance and can better resist eavesdropping attacks than the other methods. According to the performance analysis, the proposed scheme has the same performance as the ordinary schemes and does not need additional security channels. Moreover, the proposed scheme can promptly find and discard the contaminated packets, thus effectively resisting message pollution attack.

7 References

[1] Naranjo, P. G., Shojafar, M., Mostafaei, H., Pooranian, Z., & Baccarelli, E. P-sep: a prolong stable election routing algorithm for energy-limited heterogeneous fog-supported wireless sensor networks. Journal of Supercomputing, 2017, vol. 73(2), pp. 1-23. https://doi.org/10.1007/s11227-016-1785-9

[2] Li, X., Tao, X., & Li, N. Energy-efficient cooperative mimo-based random walk routing for wireless sensor networks. IEEE Communications Letters, 2016, vol. 20(11), pp. 2280-2283. https://doi.org/10.1109/LCOMM.2016.2599183

[3] Yuvaraja, M., & Sabrigiriraj, M. Fault detection and recovery scheme for routing and lifetime enhancement in wsn. Wireless Networks, 2017, vol. 23(1), pp. 1-11. https://doi.org/10.1007/s11276-015-1141-7

[4] Logambigai, R., & Kannan, A. Fuzzy logic based unequal clustering for wireless sensor networks. Wireless Networks, 2016, vol. 22(3), pp. 945-957. https://doi.org/10.1007/s11276-015-1013-1

[5] Orojloo, H., & Haghighat, A. T. A tabu search based routing algorithm for wireless sensor networks. Wireless Networks, 2016, vol. 22(5), pp. 1-14. https://doi.org/10.1007/s11276-015-1060-7

[6] Ferng, H. W., & Khoa, N. M. On security of wireless sensor networks: a data authentication protocol using digital signature. Wireless Networks, 2016, vol. 23(4), pp. 1-19.

[7] Guo, P., Liu, X., Cao, J., & Tang, S. Lossless in-network processing and its routing design in wireless sensor networks. IEEE Transactions on Wireless Communications, 2017, vol. 99, pp. 1-1. https://doi.org/10.1109/TWC.2017.2724516

[8] Rao, V., & Kar, S. Energy efficient routing in wireless sensor networks via circulating operator packets. Wireless Networks, 2018, pp. 1-18.

[9] Zhu, Y. H., Chi, K., Tian, X., & Leung, V. C. M. Network coding-based reliable ipv6 packet delivery over Ieee 802.15.4 wireless personal area networks. IEEE Transactions on Vehicular Technology, 2016, vol. 65(4), pp. 2219-2230. https://doi.org/10.1109/TVT.2015.2419082

[10] Gomez, C., Paradells, J., Bormann, C., & Crowcroft, J. From 6lowpan to 6lo: expanding the universe of ipv6-supported technologies for the internet of things. IEEE Communications Magazine, 2017, vol. 55(12), pp. 148-155. https://doi.org/10.1109/MCOM.2017.1600534

[11] Zhu, Y. H., Qiu, S., Chi, K., & Fang, Y. Latency aware ipv6 packet delivery scheme over ieee 802.15.4 based battery-free wireless sensor networks. IEEE Transactions on Mobile Computing, 2017, vol. 16(6), pp. 1691-1704. https://doi.org/10.1109/TMC.2016.2601906

[12] Thang, V. C., & Tao, N. V. A performance evaluation of improved ipv6 routing protocol for wireless sensor networks, 2016, vol. 8(12), pp. 18-25.

8 Author

Zhaoyan Li and **Chengfang Zhao** are with the School of Computer & Software Engineering, Xihua University, Chengdu 610039, Sichuan, China.

Article submitted 14 June 2018. Resubmitted 16 July 2018. Final acceptance 23 July 2018. Final version published as submitted by the authors.