Computer Life (CPL) ISSN: 1819-4818
DELIVERING QUALITY SCIENCE TO THE WORLD

# A Survey of Multipath Secure Routing in WSN

Huixing Chen

Merchant Marine College, Shanghai Maritime University, China

18826070682@163.com

---

*Abstract: In The security of routing in WSN involves keys management, authentication, energy saving, congestion and many other factors. We summarize classify and compare the existing multipath secure routing protocols according to the core secure schemes used by them and emphatically introduced and analyzed the important and typical ones among them. Lastly this paper proposed some problems which were worth further studying in multipath secure routing area in WSN.*
*Keywords: Multipath routing, Security, Wireless sensor networks*

---

## 1. INTRODUCTION

Wireless sensor networks (WSNs) have been widely used in environmental monitoring due to their low power consumption, low cost, distributed and self-organizing characteristics [1-2]. Due to the multi-hop forwarding data transmission mechanism and the self-organizing networking mechanism, each node in the network needs to participate in the discovery, establishment and maintenance of routes. These features make wireless sensor networks very risky to attack and data anomalies. . In the fields of military monitoring, medical care, security prevention and monitoring, the information collected by sensor networks is highly sensitive. Since these applications require real-time and reliable information to provide services, it is essential to ensure that information is secure during acquisition and transmission. In order to enhance the reliability, fault tolerance and stability of the network, the method of providing multipath routing has been proposed by many researchers. However, because the multipath routing method makes data available in multiple locations, it introduces additional security issues, which gives attackers more opportunities to destroy data. Therefore, it is very important to protect wireless sensor networks from malicious attacks in sensitive environments.

At present, the WSN multi-path routing security problem has not received enough attention. Many routing protocols are designed only to reduce the data packet loss rate, save energy consumption and extend the life cycle of the network. Focus [3-7]. Multi-path routing can effectively prevent information selection and forwarding attacks, and can overcome the problem that single-path routing needs to be repaired after the network communication link is disconnected. Multipath routing is widely used to extend the life cycle of the network and improve the quality of service (QoS) of the network. Multipath routing protects data information from attacks by reducing the chances that

packets are modified or discarded by malicious sensor nodes [8]. In addition, the lightweight security mechanism can adapt to multi-path routing technology, which further improves the security of data transmission in WSN by mitigating the impact of network attacks [9].

In wireless sensor networks, achieving secure communication between node information is a challenging problem. Domestic and foreign scholars have done a lot of research on WSN multi-path secure routing, and have achieved fruitful research results. This article reviews the latest WSN multipath secure routing protocol. We discussed the drivers, security requirements, and WSN network attacks for the development of multipath routing protocols. WSN routing protocols are vulnerable to a variety of attacks, such as forged routing information, witch attacks, wormhole attacks, sinkhole attacks, and hello flood attacks. These attacks can affect the performance of the network and shorten the life cycle of the network. Repeatedly discarding, stealing or tampering with network information, destroying the entire network and causing irreparable damage to users [10-12].

## 2. MULTIPATH SECURE ROUTING REQUIREMENTS

Routing is the basic operation in WSNS. It is used to establish communication links between sensor nodes and implement packet delivery. Most security key areas, such as data security aggregation, secure location, intrusion detection, key management, etc., rely on routing schemes to exchange data and support their operations [13]. A routing path is usually a single path between a resource node and a destination node. Data loss is unacceptable in sensitive areas, such as military and medical environments, and their tasks are highly dependent on accurate information. Therefore, the availability of data and the reliability of communication are necessary. Multipath routing also faces some problems with single path routing. Before designing a secure routing protocol, we should first consider the cause of the security problem in the multipath routing process. Only in this way can the researcher propose a suitable design. The reasons are as follows:

(1) Data redundancy

Multipath routing introduces data redundancy into the network when a redundant routing policy is taken. In redundant routing, data is available at multiple locations, giving broadcasters more opportunities to disseminate information. When attacking different nodes at the same time, the opponent has a higher probability of corrupting the data packet, which is unacceptable in sensitive applications, because the interception or modification of critical data may cause the application operation to be damaged or even endanger the life of the person.

(2) Routing attacks

In multipath routing, attacks can seriously affect the route discovery process [14] and give the intruder the opportunity to control the establishment of routes. Attacks can affect the discovery phase of a routing path in a variety of ways. The attack has been analyzed in detail in the literature [15-20]. A hello or sybil attack allows the adversary to participate in different routing paths and trade off the data transfer alternate path in this way. To make matters worse, the adversary can listen for communication between nodes and modify the routing control packet to affect the discovery of alternate paths and create routing loops and dead ends. By controlling routing operations, the adversary can reduce overall network performance.

(3) Network life cycle

Energy optimization is a major problem in wireless sensor network applications. Since different scenarios have different network sizes and applications, it is very difficult to ensure a optimized energy system using a unified protocol, and the lifetime of the wireless sensor network is less than the optimal time due to the premature occurrence of energy holes. Most routing algorithms usually consider nodes, cluster internal energy, or energy optimization of the entire network. The bottom-up approach is not suitable for large-scale and large sensor nodes. The classic wireless sensor network routing algorithm is the low energy adaptive clustering algorithm (LEACH) [21]. In order to avoid the occurrence of energy holes in wireless sensor networks, the network is positioned as part of the wireless sensor network network energy optimization, rather than as a final goal.

## 3. MULTIPATH SECURE ROUTING PROTOCOL

Multi-path routing can effectively improve the delivery success rate of data messages and balance node energy consumption to prolong the lifetime of nodes. At the same time, multipath routing is also an effective defense method for selective forwarding attacks [22]. The research on the security problem of multipath routing in wireless sensor networks can be traced back to the SPINS protocol proposed by Perrig et al. in 2002 [23]. In densely deployed wireless sensor networks, routing is the key to sending sensor node data to the base station. If the two nodes are not in the communication range of each other, the network forwards the information through the relay node. In multi-path routing, if a small number of nodes are damaged by an attack, the entire information transmission of the network is generally not affected.

Literature [24] proposed a new multi-path routing SMRP, on the basis of which SEIF [25] was designed. The difference between the multi-path routing protocol and the previous permissible intrusion-based routing protocol is that it has distributed and network inspection technologies, and does not need to submit the establishment process and security check of the multi-path routing to the server. This protocol also uses a new multi-path. The path selection plan enhances the bandwidth of the wireless sensor network while saving the energy consumption of the sensing nodes. SEIF relies on a one-way hash chain to establish a multi-path, multi-to-one propagation link tree, as well as acknowledgment of multipath routing initialization and parent node authentication; one-way hash chain provides authentication of exchange control information; Hello flood attacks and wormhole attacks use a suspicion mechanism. However, the protocol cannot be faced with a large number of external attacks. If an attacker captures a normal node, it can find information about the encrypted data store and use it to break the network confidentiality.

The routing protocol MPRASRP [26] can effectively prevent an attacker from obtaining the identity of the network node node and the base station node, so as to prevent the attacker from further controlling the data transmission processing between the two communication nodes. The traditional anonymous routing protocol is a single path problem, and the protocol proposes the idea of using multipath. The reason for ensuring node anonymity is that the identity of the source node and the destination node is encrypted with the public key of the target source node, and only the target source node can decrypt the data packet. The protocol can effectively prevent the network from being attacked by middlemen, and it is also very effective in harsh environments such as large ocean waves, but the protocol cannot prevent the network from being repeatedly attacked. MASK [27-28] also achieves security through anonymity, in which the MAC layer and the network layer exchange

information do not need to disclose the information of each node, and provide the relationship between the sending node and the receiving node and the two communication nodes. Anonymity, and the use of dynamic anonymity in the transmission of information, can prevent network eavesdropping and repeated attacks, while greatly saving energy.

The multi-path secure routing protocol based on malicious node detection [29-35] comprehensively considers the balance between network energy consumption and security, and uses the encryption and authentication process combined with symmetric key and asymmetric key. The negotiation mechanism is used to effectively identify malicious nodes and prevent nodes from sending data to malicious nodes. Once a malicious node is determined, the node ID is blacklisted. When the route is guaranteed, the route can be discovered in time, and the topology of the wireless sensor network is not exposed, which can effectively resist the threat against routing security. For the delay problem, the protocol introduces a dual queue model at the node, which effectively controls the delay of network transmission.

Connectivity is an important concept in multi-hop routing protocols. The literature [36] extends K-connectivity and introduces the K-X-connectivity concept. The protocol also extends the DSR algorithm to use extreme digital signature authentication when exchanging packets. In order to ensure the security of the route, the protocol requires that the node must be able to authenticate other nodes when establishing the route; the forged packets must be detected before reaching the base station; the node also monitors the behavior of the neighbor nodes; the protocol uses the watchdog mechanism To detect that the node does not forward packets; the protocol can avoid wormhole attacks [37].

For the DDoS attack of the broadcast authentication protocol, the literature [38] designed a defense method. The protocol is based on DBP-MSP and secure routing, and the broadcast status table is introduced. The base station updates the broadcast status table according to the node information, and the receiver can determine the solution for solving the DDoS attack by the information returned by the base station through the search table. The key chain scheme is also introduced. At intervals, the base station sends a one-way keychain to the sender, reducing the sender's storage and computational burden.

Literature [39] proposed the concept of security policy. Routing Protocol Research Designers and administrators have the ability to access sensor node resources. Routing security policies are based primarily on trust, tasks, and pre-keys. Protocols use IBC to encrypt node and group identities; and these policies can be adaptively sensed. Network conditions and external interference factors. Efficient processing strategies are set for witch attacks, wormhole attacks, and so on. In response to two newer attacks, namely, non-cooperation between members of wireless sensor networks and hidden packet loss by malicious nodes, the literature [40] proposes a new self-healing community mechanism to solve these two attacks. The core idea is to mitigate the selfish behavior of the attacker and the actions of the malicious node by decentralizing the network service inquiry to the neighbor node society. The protocol is based on a large number of relay nodes to monitor the data packets in real time during transmission. The network simulation experiments prove that the protocol has strong security.

## 4. RESEARCH PROSPECT OF WSN MULTIPATH SECURE ROUTING PROTOCOL

Researchers at home and abroad have done a lot of work on wireless sensor network security routing, and have obtained rich research results. Many effective multi-path security routing mechanisms have been proposed. However, the following problems still exist in the existing research work and need further research and resolution:

(1) How to further extend the life cycle of wireless sensor networks while ensuring the security of network data transmission.

(2) Compared with wireless sensor networks with stationary nodes, the characteristics of network discontinuity and frequent topology changes caused by the mobility of nodes in mobile sensor networks pose new requirements and challenges for their routing security mechanisms. However, the existing research work is mainly aimed at wireless sensor networks with node stationary. In the future, further research on multipath routing security of mobile sensor networks is needed.

## REFERENCES

[1] Romer K, Mattern F. The design space of wireless sensor networks[J]. IEEE wireless communications, 2004, 11(6): 54-61.

[2] Al-Karaki J N, Kamal A E. Routing techniques in wireless sensor networks: a survey[J]. IEEE wireless communications, 2004, 11(6): 6-28.

[3] De S, Qiao C, Wu H. Meshed multipath routing: An efficient strategy in sensor networks[C]//2003 IEEE Wireless Communications and Networking, 2003. WCNC 2003. IEEE, 2003, 3: 1912-1917.

[4] Sohrabi K, Gao J, Ailawadhi V, et al. Protocols for self-organization of a wireless sensor network[J]. IEEE personal communications, 2000, 7(5): 16-27.

[5] Ganesan D, Govindan R, Shenker S, et al. Highly-resilient, energy-efficient multipath routing in wireless sensor networks[J]. ACM SIGMOBILE Mobile Computing and Communications Review, 2001, 5(4): 11-25.

[6] Gurav A A, Nene M J. Optimal Path Identification using Ant Colony Optimisation in Wireless Sensor Network[J]. Computer Science & Information Technology,© CS & IT-CSCP, 2013, 2013: 223-232.

[7] Fan Y, Zhong G, Lu S, et al. GRAdient broadcast: a robust data delivery protocol for large scale sensor networks[J]. Wireless Networks, 2005, 11(3): 285.

[8] Dong J, Curtmola R, Nita-Rotaru C. Secure network coding for wireless mesh networks: Threats, challenges, and directions[J]. Computer Communications, 2009, 32(17): 1790-1801.

[9] Nasser N, Chen Y. SEEM: Secure and energy-efficient multipath routing protocol for wireless sensor networks[J]. Computer communications, 2007, 30(11-12): 2401-2412.

[10] Deng J, Han R, Mishra S. INSENS: Intrusion-tolerant routing for wireless sensor networks[J]. Computer Communications, 2006, 29(2): 216-230.

[11] Li H, Lin K, Li K. Energy-efficient and high-accuracy secure data aggregation in wireless sensor networks[J]. Computer Communications, 2011, 34(4): 591-597.

[12] Karimi H, Medhati O, Zabolzadeh H, et al. Implementing a reliable, fault tolerance and secure framework in the wireless sensor-actuator networks for events reporting[J]. Procedia Computer Science, 2015, 73: 384-394.

[13] Chen H, Lou W, Wang Z, et al. Securing DV-Hop localization against wormhole attacks in wireless sensor networks[J]. Pervasive and Mobile Computing, 2015, 16: 22-35.

[14] Mavropodi R, Kotzanikolaou P, Douligeris C. SecMR–a secure multipath routing protocol for ad hoc networks[J]. Ad Hoc Networks, 2007, 5(1): 87-99.

[15] Wang Y, Attebury G, Ramamurthy B. A survey of security issues in wireless sensor networks[J]. IEEE Communications Surveys & Tutorials ,2006,. 8 (2): 2–23.

[16] Karlof C, Wagner D. Secure routing in wireless sensor networks: Attacks and countermeasures[C]//Proceedings of the First IEEE International Workshop on Sensor Network Protocols and Applications, 2003. IEEE, 2003: 113-127.

[17] Wood A D, Stankovic J A. Denial of service in sensor networks[J]. computer, 2002, 35(10): 54-62.

[18] Wood A D, Stankovic J A. A taxonomy for denial-of-service attacks in wireless sensor networks[J]. Handbook of sensor networks: compact wireless and wired sensing systems, 2004: 739-763.

[19] Zhu S, Setia S, Jajodia S. LEAP+: Efficient security mechanisms for large-scale distributed sensor networks[J]. ACM Transactions on Sensor Networks (TOSN), 2006, 2(4): 500-528.
[20] Zia T, Zomaya A. Security issues in wireless sensor networks[C]//2006 International Conference on Systems and Networks Communications (ICSNC'06). IEEE, 2006: 40-40.
[21] Masdari M, Bazarchi S M, Bidaki M. Analysis of secure LEACH-based clustering protocols in wireless sensor networks[J]. Journal of Network and Computer Applications, 2013, 36(4): 1243-1260.
[22] Yang W, WANG R, CHENG X. Improved multipath routing with WNN for the open networks[J]. The Journal of China Universities of Posts and Telecommunications, 2008, 15(2): 107-113.
[23] Perrig A, Szewczyk R, Tygar J D, et al. SPINS: Security protocols for sensor networks[J]. Wireless networks, 2002, 8(5): 521-534.
[24] Zin S M, Anuar N B, Kiah M L M, et al. Survey of secure multipath routing protocols for WSNs[J]. Journal of Network and Computer Applications, 2015, 55: 123-153.
[25] Ouadjaout A, Challal Y, Lasla N, et al. SEIF: secure and efficient intrusion-fault tolerant routing protocol for wireless sensor networks[C]//2008 Third International Conference on Availability, Reliability and Security. IEEE, 2008: 503-508.
[26] Fanian A, Berenjkoub M, Saidi H, et al. A high performance and intrinsically secure key establishment protocol for wireless sensor networks[J]. Computer networks, 2011, 55(8): 1849-1863.
[27] Guermazi A, Abid M. An efficient key distribution scheme to secure data-centric routing protocols in hierarchical wireless sensor networks[J]. Procedia Computer Science, 2011, 5: 208-215.
[28] Elhoseny M, Elminir H, Riad A, et al. A secure data routing schema for WSN using elliptic curve cryptography and homomorphic encryption[J]. Journal of King Saud University-Computer and Information Sciences, 2016, 28(3): 262-275.
[29] Long J, Liu A, Dong M, et al. An energy-efficient and sink-location privacy enhanced scheme for WSNs through ring based routing[J]. Journal of parallel and Distributed computing, 2015, 81: 47-65.
[30] Sun B, Li C C, Wu K, et al. A lightweight secure protocol for wireless sensor networks[J]. Computer communications, 2006, 29(13-14): 2556-2568.
[31] Rahman S M M, El-Khatib K. Private key agreement and secure communication for heterogeneous sensor networks[J]. Journal of Parallel and Distributed Computing, 2010, 70(8): 858-870.
[32] Jeba S V A, Kumar R S. Reliable anonymous secure packet forwarding scheme for wireless sensor networks[J]. Computers & Electrical Engineering, 2015, 48: 405-416.
[33] Sánchez-Carmona A, Robles S, Borrego C. PrivHab+: A secure geographic routing protocol for DTN[J]. Computer Communications, 2016, 78: 56-73.
[34] Pathak G R, Patil S H. Mathematical Model of Security Framework for Routing Layer Protocol in Wireless Sensor Networks[J]. Procedia Computer Science, 2016, 78: 579-586.
[35] Shamshirband S, Patel A, Anuar N B, et al. Cooperative game theoretic approach using fuzzy Q-learning for detecting and preventing intrusions in wireless sensor networks[J]. Engineering Applications of Artificial Intelligence, 2014, 32: 228-241.
[36] Zin S M, Anuar N B, Kiah M L M, et al. Survey of secure multipath routing protocols for WSNs[J]. Journal of Network and Computer Applications, 2015, 55: 123-153.
[37] Dong J, Ackermann K, Nita-Rotaru C. Secure group communication in wireless mesh networks[J]. Ad Hoc Networks, 2009, 7(8): 1563-1576.
[38] Prabha R, Krishnaveni M, Manjula S H, et al. QoS Aware Trust Metric based Framework for Wireless Sensor Networks[J]. Procedia Computer Science, 2015, 48: 373-380.
[39] Cheikhrouhou O. Secure group communication in wireless sensor networks: a survey[J]. Journal of Network and Computer Applications, 2016, 61: 115-132.
[40] Mohemed R E, Saleh A I, Abdelrazzak M, et al. Energy-efficient routing protocols for solving energy hole problem in wireless sensor networks[J]. Computer Networks, 2017, 114: 51-66.