International Journal of Contemporary Research in Computer Science and Technology (IJCRCST) ISSN: 2395-5325
Volume 3, Special Issue 1 (February '2017)
Special Issue on 1st National Conference on Advanced Computing and Communication Technologies,
Conference held at Siri PSG Arts and Science College for Women, Sankari,Tamilnadu,India.

ANALYSIS OF MULTIPATH RELIABLE ROUTING PROTOCOL SECURITY FOR WSN

S. Boopathi,
Research scholar,
Periyar university,
Salem, Tamilnadu

Dr. A.SenthilKumar,
Assistant Professor,
Department of Computer Science,
Arignar Anna Government Arts College,
Namakkal,Tamilnadu.

Abstract: Security in Wireless Sensor Networks is the major concern when they are used in military and national applications. Traditional routing protocols are designed for attaining maximum throughput but they cannot guarantee security and reliability.This article presents the study of major security attacks in WSNs and the level of Multipath Secure Reliable Routing's resistance against the security attacks. Different types of security attacks and the counter-measures of MSR to prevent those attacks are presented under three broad categories: Attacks completely prevented by MSR, attacks which can be prevented by reducing their effect and attacks which needs to be handled by different means.

Key words: Security, Wireless sensor networks, Routing, Multiple Reliable Routing

I.INTRODUCTION

A Wireless Sensor Network (WSN) is a collection of wireless sensor nodes forming a temporary network without the aid of any established infrastructure or centralized administration. In such an environment, due to the limited range of each node's wireless transmissions, it may be necessary for one sensor node to ask for the aid of other sensor nodes in forwarding a packet to its destination, usually the base station. WSN node gathers sensor data and passes information to the coordinator. Correspondingly, the coordinator performs appropriate control action as necessary. The sensor node transmits the data to the coordinator directly or via one or more routers. The challenge in a typical industrial environment is to ensure effective transfer of data from one place to another, in a reliable manner, within the allowable delay, with the least no of hops and minimum packet overhead amidst congestion, collision, link- failures, link-delays, etc.

WSN have been vulnerable to numerous security attacks. Increased applications have resulted in increased deployment especially in the areas of defense, surveillance, environmental monitoring and healthcare. Sensitive information transmitted across the sensors are prone to attacks due to the wireless nature of communication. The impact of attacks can lead to reduced lifetime of the sensors, performance drops and information misuse. In case of health care applications, the impact can be deadly and life threatening. Hence security is one of the most crucial aspects of Wireless Sensor Networks which needs to be addressed so as to reduce or remove any impact of various kinds of attacks be it internal or external. There are various attacks on the Routing Layers in WSN which can be categorized into Active and Passive attacks. Most of the attacks on Routing Layers Are Active in nature. Some of the active attacks, along with the solution available to mitigate the impact of these attacks on the routing protocols are discussed. The Section has been organized with listing of Sinkhole, Selective Forwarding, Gray hole, Wormhole and Blackhole Attacks. Against each attack, the related work on improving performance under the attack is discussed.

II. TYPICAL ATTACKS ON WSNS

In the preliminary stage of routing protocol design, people concentrated mainly on improving the success ratio of data submission, transmission delay time reduction, consuming less energy by the nodes and to prolong the survival time of the network. But, security was not taken into consideration, which poses serious threat to WSN.

Attacks can be classified into outsider attacks and insider attacks. Outsider attacks are where the attacker has no special access to the sensor network, and the insider attacks are where an authorized participant in the sensor network has gone badly. Insider attacks can be either compromised sensor nodes running malicious code or external devices use stolen key material and data from legitimate nodes to attack the network.

The following is the brief description of the different attacks on WSNs

1. **Hello flood attack:** With a laptop, an adversary can broadcast this HELLO message and all nodes in the sensor network might believe that the compromised node belongs to their neighborhood and convince every node in the network that they are the neighbor.

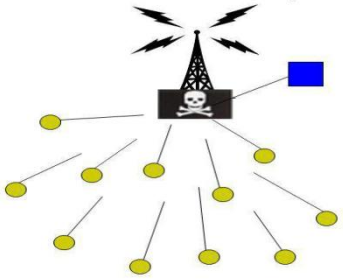

Figure 1. Hello Flood attack

2. **Blackhole attack:** A type attack in which a router that is supposed to relay packets instead discards them. This usually occurs from a router becoming compromised from a number of different causes.

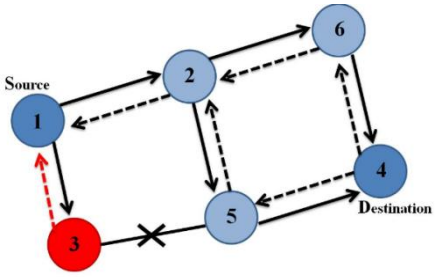

Figure 2. Black hole attack

3. **Selective forwarding attack:** A malicious node refuses to route certain messages or drops them. However, such nodes can selectively forward the packets with some probability.

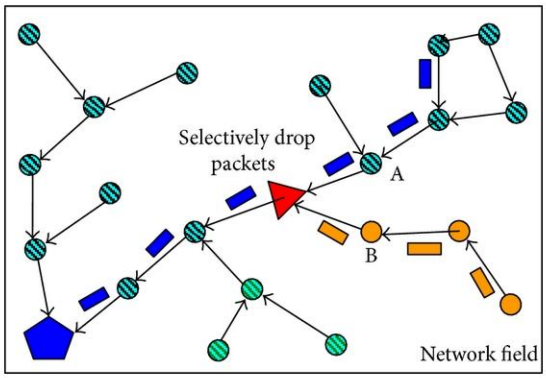

Figure 3. Selective forwarding attack

4. **Acknowledgement spoofing attack:** The attacker spoofs the acknowledgment convincing the sender that a weak limnk may be strong or a dead node is alive. This result in lost packets when travelling along such links.
5. **Replay attack:** The attacker targets the routing information exchanged between nodes by spoofing, altering, or replaying routing information. Adversaries may be able to create routing loops, attack, or repel network traffic, extend or shorten source routes, generate false error messages, partition the network, and/or increase end to end latency.
6. **Sinkhole attack:** An adversary tries to attract almost all the traffic toward the compromised node. (The pathpresented through themalicious node appears to be the best available route for the nodes to communicate)
7. **Wormhole attack:** An adversary tunnels messages received in one part of the network over a low latency link, to another part of the network where the messages are then replayed. (Wormholes are dangerous because they can do damage without even knowing the network.)
8. **Sybil attack:** A single adversary node presents multiple identities to all other nodes in the WSN, which may affect data aggregation, voting or disjoint path routing.

III. WSN ATTACKS AND DEFENSE BY MSR:

MSR defense against WSN can be classified into three broad categories:

1. Attacks prevented by MSR:

These attacks are prevented by one or more of the three components of MSR.

- *Hello flood attack:* MSR sends packets by multiple paths and any number of packets can be used to construct the original packet, a single attacker cannot compromise all the paths.

Passive Acknowledgment (PACK) refers to the sender passively listens after finishing the message transmission to confirm that the message has been received by the destination called indirect overhearing

- *Black hole attack:* By enhanced passive acknowledgement scheme, black hole attack can be prevented.
- *Selective forwarding attack:* Similar to Black hole attack, Selective forwarding attack can also be prevented by enhanced passive acknowledgement scheme.
- *Acknowledgement spoofing attack:* This attack can also be prevented by enhanced passive acknowledgement scheme.
- *Replay attack:* This attack can also be prevented by enhanced passive acknowledgement scheme.

In all of the above attacks, using multiple paths and erasure coding significantlydegrades the ability of the attacker to disable a connection between a source and a destination. This remains true for more than one attacker.

2. Attacks whose effect reduced by MSR:

The effect is reduced by one or more of the three components of MSR namely

- Sinkhole attack
- Wormhole attack

Even if these attacks cannot be detected, using multipath routing and erasure coding significantly reduces the attacker ability to completely disrupt the communication between two nodes

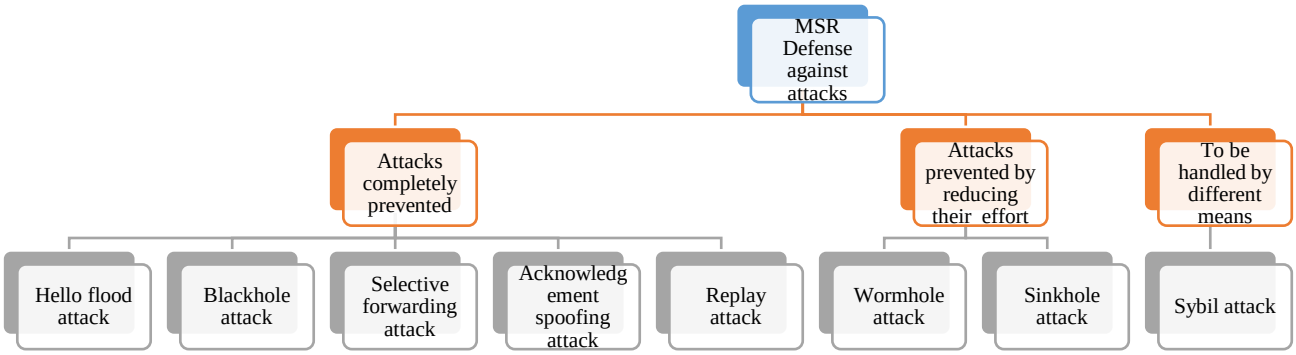

Figure 4. MSR attack analysis

3. Attacks that require further processing:

Sybil attack cannot be prevented by MSR but the same can be extended to defend against this attack using different techniques including registration, authentication, sharing random keys, and RF position verification.

IV.CONCLUSION

We presented the different types of attacks that affects the security of the WSN. MSR as a protocol achieve high security attack level and provides more reliability for WSN. Being widely used in military, environmental, health and commercial applications, WSN security becomes crucial. These networks are inherently from traditional wireless network as well as WSNs.This article summarizes the attack and their taxonomy and also an attempt has been made to explore the security mechanisms widely used to handle those attack. Another direction is the analysis of MSR performance under specific attacker assumption.

V.REFERENCES

[1]Chun-Chuan Yang, Li-Pin Tseng, 2007. 'Fisheye zone routing protocol: A multi-level zone routing protocol for mobile ad hoc networks', Journal in Computer Communication.

[2]Celia John, and CharuWahi, Security Analysis of Routing Protocols for Wireless Sensor Networks, International Journal of Applied Engineering Research ISSN 0973-4562 Volume 11, Number 6 (2016) pp 4235-4242

[3]SabithaRamakrishnan and C. Bharath, FDRRP - A Reliable Routing Protocol for Wireless Sensor Networks, Middle-East Journal of Scientific Research 23 (Sensing, Signal Processing and Security): 392-397, 2015

[4] Wang, L. and S. Olariu, 2004. 'A two-zone hybrid routing protocol for mobile ad hoc networks', IEEE Transactions on Parallel and Distributed Systems 15(12): 1105-1116.

[5] A. Perrig et al., "SPINS: Security Protocols for Sensor Networks," Wireless Networks, vol. 8, 2000, pp. 521–34.

[6] I. Akyildiz, X. Wang and W. Wang. "Wireless mesh networks: a survey". Computer Networks, vol. 47, no. 4, 2005, pp. 445-487.

[7] Islam T. Almalkawi, Manel Guerrero Zapataand Jamal N. Al-Karaki, A Secure Cluster-Based Multipath Routing Protocol for WMSNs

[8] J. Eriksson, M. Faloutsos and S. Krishnamurthy. "Peernet: Pushing peer-2-peer down the stack". In Proc. of IPTPS, 2003.

[9] C. Perkins and E. Royer. "Ad hoc on-demand distance vector routing".2nd IEEE Workshop on Mobile Computing Systems and Applications, New Orleans, LA, United States, 1999,

[10] Jingsha He, Bo Zhou and Ruohong Liu, Analysis of Typiical Secure Protocols in WSN, International Journal of Security and its applications, Vol.8,No.6 (2014), pp41-50

[11] D. B. Johnson and D. A. Maltz. "Dynamic source routing in ad hoc wireless networks". In Mobile Computing, vol. 353, 1996, pp. 153-181.