Volume 4, Issue 11, November 2014 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

# Protective Mechanism to Avoid Warm hole and Sink-hole Attack in Wireless Ad hoc Network: A Survey

**Rajani Patil*, Santosh Biradar**
Department of Computer Science,
Pune University, Maharashtra, India

*Abstract*— ***Wireless sensor network is autonomous and infrastructure less network. Different types of WSN applications are developed. Wireless sensor network is particularly vulnerable due to its fundamental characteristics, such as open medium, dynamic topology, distributed cooperation, and constrained capability. Routing plays an important role in the security of the entire network. Secure transmission of information in wireless adhoc environment is an important concern. Any attacker receive wireless signal by using transceiver and without being detected. Objective of this paper is to propose new secure unobservable routing protocol where attacker get blocked while making spoofing or DOS attacks. Only unobservant message could be collected by attacker. Our protocol should protect privacy information among network and detect and block attacking nodes through trust mechanism.***

***Keywords— Sensor networks, security, secure unobservable routing protocol, WSN, spoofing***

## I. INTRODUCTION

A wireless sensor network is collection of thousands of tiny wireless sensor nodes for data communication purpose. These sensor nodes cooperate with each other to accomplish data transmission. Numerous applications built in WSN like security, inventory tracking, automotive control, surveillance, health monitoring and other civil tasks, bridge monitoring, home automation in the recent years. Sensors are inexpensive, low power devices, which have limited resources.

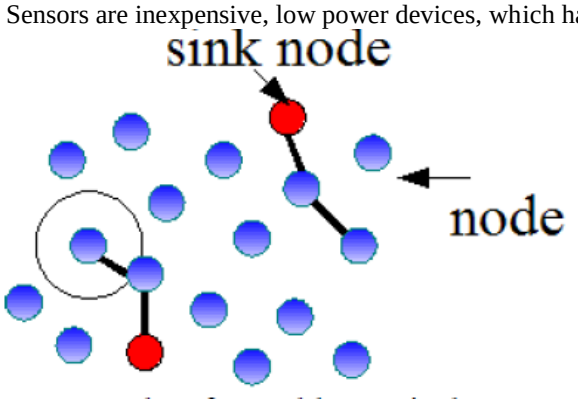


Figure 1: WSN Architecture

Figure 1 shows system architecture of wireless sensor network. The number of sensor node in WSN are usually large. Each node contains a power unit, a processing units, a storage units, sensing unit and wireless transmitter or receiver. The Sensor nodes communicate with each other through simultaneous transmission of data from one node to another node. As transmitter range is limited, data must be forwarded in multiple host in order to reach remote node which is at long distance from originating source node. Cost of sensor node depends on complexity of applications.The sensors are still available at low cost. Generally, star topology is used in WSN.

### *A. SECURITY REQUIREMENTS IN WSN*

WSNs are special kind of Ad-hoc networks. Security services in WSNs are required to protect the information and resources from attacks and misbehavior. The security requirements in WSNs include:

1. Availability: Availability ensures that the desired network services are available even in the presence of denial-of-service attacks.
2. Authorization: Authorization ensures that only authorized sensors can be involved in providing information to network services.
3. Privacy: Privacy prevents adversaries from obtaining information that may have private content.
4. Authentication: which ensures that the communication from one node to another node is genuine, that is, a malicious node cannot masquerade as a trusted network node.

 

5. Anonymity[1] : Anonymity hides the source of the data. It is a service that can help with data confidentiality and privacy.
6. Unlinkability[1]: Unlinkability of two or more Item of identity (IOI) means these IOIs are no more or no less related from the assailant's perspective.
7. Unobservability[1]: Unoservability of IOI express that whether it exists or not is undefined to all random subjects, and subjects identified with this IOI are nameless to all other related subjects. It is of two types :
   - Content Unobservability, referring to no useful information can be extracted from content of any message
   - Traffic Pattern Unobservability, referring to no useful information can be obtained from frequency, length, and source-destination patterns of message traffic.

8. Resilience: Resilience sustains the network functionalities when a portion of nodes are compromised by the attacks.
9. Confidentiality: Confidentiality ensures that a given message cannot be understood by anyone other than the desired recipients.
10. Integrity: Integrity ensures that a message is not modified during the transmission.
11. Nonrepudiation: Nonrepudiation denotes that a node cannot deny sending a message, it has previously sent.
12. Self Organization: Wireless sensor networks are spatial kind of Ad-hoc networks in which every sensor node should be self healing and self organizing. The dynamic nature of a WSN makes it sometimes impossible to deploy any preinstalled shared key mechanism among the nodes and the base station .
13. Time Synchronization: Most sensor network applications rely on some form of time synchronization. Sensors may wish to compute the end-to-end delay of a packet as it travels between two pair wise sensors. A more collaborative sensor network may require group synchronization for tracking applications .
14. Secure Localization: In WSN each sensor node is required to locate itself in the network accurately and automatically to identify the location of the fault.
15. Flexibility: Sensor networks will be used in dynamic battlefield scenarios where environmental conditions, threat, and mission may change rapidly. Changing mission goals may require sensors to be removed from or added to an established sensor node. Furthermore, two or more sensor networks may be fused into one, or a single network may be split in two. Key establishment protocols must be flexible enough to provide keying for all potential scenarios a sensor network may encounter.
16. Freshness: Freshness implies that the data is recent and ensures that no adversary can replay old messages. To make sure that no old messages replayed,a timestamp can be added to the packet. Sensor nodes have limited processing capability, very low storage capacity, and constrained communication bandwidth. Due to these constraints, it is difficult to directly employ the conventional security mechanisms in WSN.

### *B. SECURITY THREATS AND ATTACKS IN WSN*

1. Denial Of Service: The DOS attack tries to busy the available resource by the victim node by sending extra unnecessary packets result is other network users cant uses the available resources. DOS attacks disrupt the network as well as block the services. Strong authentication and identification is required for Prevention from the DOS attack.
2. Attack on information in transit: The information during transit may be changed, spoofed, replayed again. This node provides incorrect information to sink node.
3. Sybil attack: In WSN Sensor nodes are works together for completion of any task. Sensor nodes divide their task into subtasks and redundancy of information. In this condition node can represent to be more than one node is known as Sybil attack.
4. Blackhole attack: In this type of attack a malicious node represent as black hole to induce all the traffic in the sensor network. Once malicious node introduced into the network, then it able to do anything with packet passing between them.
5. Wormhole attack: Wormhole attack is one of the critical attacks. In this type of attack attacker records the packet coming from one location and underpass those to another location. In this attack no need to compromising a sensor node.
6. Gray hole: Gray hole is a node that selectively omits packet with certain probability causing network distraction. Gray hole may drop packets coming from (or destined to) certain specific node(s) in the network while forwarding all the packets for other nodes. In another way, gray hole may also behave maliciously for some time period by dropping all packets but may switch to normal behavior after some time. A gray hole may also illustrates a behavior having combination of the above two.
7. Jellyfish attack: In jellyfish attack, the malicious node first intrudes into the forwarding group in the network and then it unreasonably delays data packets for some amount of time before forwarding them. This results in significantly high end to- end delay and delay jitter, and thus degrades the performance of real-time applications.
8. Spoofing: This occurs when a malicious node pretends to be identity of other nodes. This will misguides a non malicious node in order to change the vision of the network topology that it can gather.

## II. LITERATURE SURVEY

### *A. ANONYMITY, UNOBSERVABILITY, PSEUDONYMITY [1]*

Based on the nomenclature of the early papers in the field, we propose a terminology which is both expressive and

 

precise. More particularly, we define anonymity, unlinkability, unobservability, pseudonymity[1] (pseudonyms and digital pseudonyms, and their attributes), and identity management. In addition, we describe the relationships between these terms, give a rational why we define them as we do, and sketch the main mechanisms to provide for the properties defined.

### *B. SELF-ORGANIZED PUBLIC KEY MANAGEMENT FOR MANET [2]*

In contrast with conventional networks, mobile ad hoc networks usually do not provide online access to trusted authorities or to centralized servers, and they exhibit frequent partitioning due to link and node failures and to node mobility. For these reasons, traditional security solutions that require online trusted authorities or certificate repositories are not well-suited for securing ad hoc networks. In this paper, we propose a fully self-organized public-key management system that allows users to generate their public-private key pairs, to issue certificates, and to perform authentication regardless of the network partitions and without any centralized services. Furthermore, our approach does not require any trusted authority, not even in the system initialization phase.

### *C. ON FLOW CORRECTION ATTACKS AND COUNTERMEASURES IN MIX NETWORKS [3]*

In this paper, we address issues related to flow correlation attacks and the corresponding countermeasures in mix networks. Mixes have been used in many anonymous communication systems and are supposed to provide countermeasures that can defeat various traffic analysis attacks. In this paper, we focus on a particular class of traffic analysis attack, flow correlation attacks, by which an adversary attempts to analyze the network traffic and correlate the traffic of a flow over an input link at a mix with that over an output link of the same mix. Two classes of correlation methods are considered, namely time-domain methods and frequency-domain methods. Based on our threat model and known strategies in existing mix networks, we perform extensive experiments to analyze the performance of mixes. We find that a mix with any known batching strategy may fail against flow correlation attacks in the sense that for a given flow over an input link, the adversary can correctly determine which output link is used by the same flow. We also investigated methods that can effectively counter the flow correlation attack and other timing attacks. The empirical results provided in this paper give an indication to designers of Mix networks about appropriate configurations and alternative mechanisms to be used to counter flow correlation attacks.

## III. PROPOSED SCHEME

The proposed scheme is consisting of procedure to develop a new secure routing protocol where attacker got blocked while making spoofing or DOS attacks. We covered following key objectives,

- ✓ Sender, intermediate and destination node cannot identified by network
- ✓ Link information also protected
- ✓ Only unobservant message could be collected by attacker
- ✓ Node can compromise easily by attacks is protected by privacy preserving routing protocol, Our protocol should protect privacy information among network
- ✓ To detect and block attacking nodes through trust mechanism.

### *A. UNOBSERVABLE ROUTING SCHEME*

we present an efficient unobservable routing scheme USOR[6] for ad hoc networks. In this protocol, both control packets and data packets look random and indistinguishable from dummy packets for outside adversaries. Only valid nodes can distinguish routing packets and data packets from dummy traffic with inexpensive symmetric decryption. The intuition behind the proposed scheme is that if a node can establish a key with each of its neighbors, then it can use such a key to encrypt the whole packet for a corresponding neighbor. The receiving neighbor can distinguish whether the encrypted packet is intended for itself by trial decryption. In order to support both broadcast and unicast, a group key and a pairwise key are needed. As a result, USOR comprises two phases: anonymous trust establishment and unobservable route discovery.

## IV. CONCLUSION

In this paper, we proposed an unobservable routing protocol USOR [6] based on group signature and ID-based cryptosystem for ad hoc networks. The design of USOR offers strong privacy protection complete unlinkability and content unobservability—for ad hoc networks. The security analysis demonstrates that USOR not only provides strong privacy protection, it is also more resistant against attacks due to node compromise. This protocol help in examining performance of USOR, which shows that USOR has satisfactory performance in terms of packet delivery ratio, latency and normalized control bytes. we propose trust based mechanism to overcome Dos, man in middle, black hole, sink hole, worm hole attacks.

## REFERENCES

[1] A. Pfitzmann and M. Hansen, “Anonymity, unobservability, and pseudonymity: a consolidated proposal for terminology,” draft, July 2000.

[2] S. Capkun, L. Buttyan, and J. Hubaux, “Self-organized public-key management for mobile ad hoc networks,” IEEE Trans. Mobile Comput., vol. 2, no. 1, pp. 52–64, Jan.-Mar. 2003.

[3] Y. Zhu, X. Fu, B. Graham, R. Bettati, and W. Zhao, “On flow correlation attacks and countermeasures in mix

 

networks," in PET04, LNCS 3424, 2004, pp. 207–225.

[4] Shao-Shan Chiang, , Chih-Hung Huang, and Kuang-Chiung Chang, "A Minimum Hop Routing Protocol for Home Security Systems Using Wireless Sensor Networks," *IEEE Transactions on Consumer Electronics*, Vol. 53, No. 4, NOVEMBER 2007.

[5] Huei-Wen Ferng,Rachmarini, D.,"A secure routing protocol for wireless sensor networks with consideration of energy efficiency/Network Operations and Management Symposium (NOMS)," 2012 IEEE .

[6] Kui Ren, Ming Gu, and Zhiguo Wan (2012) "USOR: An Unobservable Secure On-Demand Routing Protocol for Mobile Ad Hoc Networks" IEEE Trans. on Wireless Communications, vol. 11, no. 5, pp. 1922-1932.

 