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

Rajani B. Patil
Department of Computer Engineering
Dr. D.Y. Patil College of Engineering Ambi,
Pune University

Dhanashree Kulkarni
Department of Computer Engineering
Dr. D.Y. Patil College of Engineering Ambi,
Pune University

ABSTRACT
Wireless adhoc network is autonomous and infrastructure less network. Wireless ad hoc network is particularly vulnerable due to its primary characteristics, like open medium, dynamic topology, distributed cooperation, and capability constraint. 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 approach for WSN security, i.e. Secure Energy Efficient ad hoc Routing (SEEAR) that consider cost of providing security and effects on energy efficiency. Shared cryptography[3] used for providing security. In this method information is divided into multiple shares and sent over multiple disjoint paths from transmitter to receiver at different point of time. At the receiver end the original information reconstructed by combining the shares received through different paths at different point of time. In this paper, cost for security in terms of time and its effect on energy efficiency is calculated. Also simulating the different types of attacks like wormhole, sink hole attack etc.

General Terms
Security, secure transmission, routing, wireless ad hoc network, wormhole attack

Keywords
Shared cryptography, Secure energy efficient ad hoc routing

1. INTRODUCTION
A wireless sensor network is special type of wireless ad hoc network. 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 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.

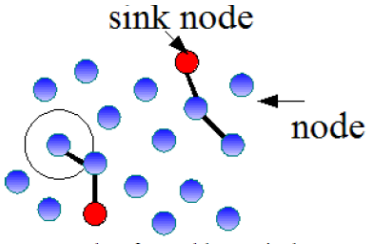

Figure 1: WSN Architecture

2. SECURITY REQUIREMENTS IN WSN [8]
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[8]:

Availability: Availability ensures that the desired network services are available even in the presence of denial-of-service attacks.

Authorization: Authorization ensures that only authorized sensors can be involved in providing information to network services.

Privacy: Privacy prevents adversaries from obtaining information that may have private content.

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.

Anonymity: Anonymity hides the source of the data. It is a service that can help with data confidentiality and privacy.

Resilience: Resilience sustains the network functionalities when a portion of nodes are compromised by the attacks.

Confidentiality: Confidentiality ensures that a given message cannot be understood by anyone other than the desired recipients.

Integrity: Integrity ensures that a message is not modified during the transmission.

Nonrepudiation: Nonrepudiation denotes that a node cannot deny sending a message, it has previously sent.

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 .

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.

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.

3. SECURITY THREATS AND ATTACKS IN WSN

Denial Of Service: The DOS attack[3] 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.

Attack on information in transit: The information during transit may be changed, spoofed, replayed again. This node provides incorrect information to sink node.

Sybil attack[3]: 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[8].

Black hole attack[8]: 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.

Worm hole attack: Wormhole attack[8] 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. It is also known as "Tunneling Attack".

Gray hole: Gray hole[3] 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.

Jellyfish attack: In jellyfish attack[8], 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.

Spoofing: Spoofing[3] 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.

4. LITERATURE SURVEY

4.1 Minimum Hop Routing Scheme[1]

A Minimum Hop Routing Protocol [1] was suggested by Shao-Shan Chiang, Chih-Hung Huang, and Kuang-Chiung Chang presents an energy-efficient, reliable and robust routing algorithm for wireless sensor networks. There are two phases are used one is routing table establishment and second is data routing phase.

4.2 Secure Disjoint Multipath Routing Scheme[3],[8]

In this schema with secret sharing is widely recognized as one of the effective routing strategies to ensure the safety of information [1],[5]. This kind of schema transfers each packet into several shares to enhance the security of transmission. Main objective is to maximize both network security and lifetime subject to the energy constraint. Designing routing strategies to bypass black holes is one of effective methods for addressing such kind of security issues. At delivering packets along disjoint multipath routes, which can be generally as follows:

- Deterministic disjoint multipath routing
- Randomly disjoint multipath routing.

Here, we discussed available security mechanism in the wireless sensor node. Basically every mechanism is build for particular application. In past, researches have designed various energy efficient schema for routing in WSN but they did not consider effect of security precautions on cost of energy spending during routing. Here we proposed routing schema that consider cost of providing security and its effect on energy efficiency. Security cost contains cryptography cost, monitoring cost and processing cost and which is time based and how much time required for cryptography, monitoring and processing. Minimum energy in term of minimum time required for providing security.

4.3 Steiner Based Security Approach[6]

Steiner Based multicast routing protocol [6] includes control on energy consumption as well as security requirements.To satisfy security requirements and control of energy consumption, Steiner-based Hierarchical Secure Multicast Routing Protocol (SHSMRP)[6] for wireless sensor network used. Here,Steiner tree and cluster network topology result is scalable and energy efficient for large group communication in WSN. Secure data communication includes data integrity, security and verifiability. Rong fan proposed Steiner based secure multicast routing protocol in two parts

- Multicast routing protocol based on Steiner tree.
- Secure multicast protocol.

This protocol includes the following five phases:

- Nodes information gathering phase
- Steiner tree construction phase
- Steiner sub-trees distribution phase
- Data delivery phase

- Steiner tree maintains phase

5. PROPOSED SCHEME

The main aim of this proposed scheme is to provide security with minimum energy cost. Here we successfully presented routing schema that consider security parameter by taking inspiration from base paper Energy efficient opportunistic routing in WSN[2]. For Security it uses secrete sharing algorithm and simulate the different attack on opportunistic routing. Mainly there are following steps comes under this context, as mentioned below.

- Obtain multiple paths using opportunistic algorithm form source to destination. (Energy Efficient path)
- Apply secrete sharing encryption algorithm at source
- Calculate cost of security
- Send encrypted data by intermediate nodes
- Destination node receives the data from different paths
- Reconstruct original message

6. OPPORTUNISTIC ROUTING TECHNIQUE (OR)[2]

It is the most famous routing algorithms for wireless networks.The Opportunistic Routing (OR) protocol[2],[8] exploits wireless networking advantages. It predicts the most useful forwarder by ranking forwarding nodes by number of hops. Opportunistic Routing forwards a packet in a sequence of nodes. A next forwarding node is determined after a previous node transmitted its packet. One node from all nodes that received the packet, which is closest to the destination, is elected as the next forwarding node. In such manner the packet approaches the destination. The path is determined during packet propagation. Each hop moves a packet farther than the hops of the best possible predetermined route After that all path Calculating there energy cost. Finally, list of paths and energy required for that path select paths that requires minimum energy.

7. SHARED CRYPTOGRAPHY ALGORITHM [3]

In this Project for security purpose secretes sharing algorithm [3] is used. That contains following steps:

- The sending node generates n unique shares from the original information by masking the original one repeatedly with each individual mask.
- Next the sending node starts sending all n shares to the destination using as many possible disjoint paths asynchronously i.e.no two shares are sent simultaneously.

Now at the destination any k nos. of received shares (assumed that the destination node has received at least k shares as n nos. of shares are been transmitted and n is larger than k) are logically ORed to reconstruct the original information.

8. CONCLUSION

In this paper, various energy efficient schema for routing in WSN are presented but they did not consider effect of security on cost of energy spending during routing. The proposed schema use secure energy efficient routing technique[5] that simulate different type of attacks and secure routing by applying secret sharing encryption and decryption algorithms. It also considers cost of providing security and its effect on energy efficiency. Secrete sharing algorithm[3] is used for providing security to data over communication within sensor nodes. This algorithm contains different parts like mask creation, shares construction and reconstruction. Hence, the proposed scheme provide defense against wormhole and sink-hole attacks. As cost of security depend on trust mechanism, the security cost can be calculated with respect to specific attack.

9. REFERENCES

[1] 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.

[2] Xufei Mao Shaojie Tang, Xiaohua Xu Xiang-Yang Li, and Huadong Ma, “Energy-Efficient Op-portunistic Routing in Wireless Sensor Networks,” IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, VOL. 22, NO. 11, NOVEMBER 2011.

[3] A Novel Security Scheme for Wireless Adhoc Network, Abhijit Das Soumya Sankar Basu Atal Chaudhuri, 978-1-4577-0787-2/11 IEEE 2011.

[4] 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 .

[5] Anfeng Liu, Zhongming Zheng , Chao Zhang, Zhigang Chen, and Xuemin (Sherman) Shen,“Secure and Energy-Efficient Disjoint Multipath Routing for WSNs,” IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY, VOL. 61, NO. 7, SEPTEMBER 2012.

[6] Rong Fan, Jian Chen, Jian-Qing Fu, Ling-Di Ping,,“A Steiner-Based Secure Multicast Routing Protocol for Wireless Sensor Network/Parallel and Distributed Systems,” IEEE Transactions on (Volume:PP , Issue: 99), April 2013.

[7] Anhtuan Le, Jonathan Loo, Aboubaker Lasebae, Alexey Vinel, Yue Chen, and Michael ChaiThe, Impact of Rank Attack on Network Topology of Routing Protocol for Low-Power and Lossy Networks. IEEE SENSORS JOURNAL, VOL. 13, NO. 10, OCTOBER 2013.

[8] Salwa Aqeel Mahdi, Mohamed Othman, Hamidah Ibrahim, Jalil Md. Desa and Jumat Sulaiman, “PROTOCOLS FOR SECURE ROUTING AND TRANSMISSION IN MOBILE AD HOC NETWORK: A REVIEW,” Journal of Computer Science 9 (5): 607-619, 2013, ISSN 1549-3636.