A Review of Routing Attacks in MANET and WSN

[1]Bikram Ballav, [2]Gayatree Rana
[1] M Tech , [2] M Tech
[1,2] Department of CSE,
ITER, Siksha 'O' Anusandhan University, Bhubaneswar , India

Abstract* - A Mobile Ad hoc Network (MANET) consists of a collection of wireless mobile nodes that are capable of communicating with each other without the use of a network infrastructure. Wireless Sensor Networks (WSN) have become a growing area of research and development due to the tremendous number of applications that can greatly benefit from such systems and has lead to the development of tiny, cheap, disposable and self-contained battery powered computers, known as sensor nodes or ―motes‖, which can accept input from an attached sensor, process this input data and transmit the results wirelessly to the transit network. Routing is a basic step for data exchange. In wireless ad-hoc networks each node acts as a router and executes a routing protocol. Wireless ad-hoc networks are highly resource constrained in terms of network topology, memory and computation power. The reliable data transfer is a difficult task in mobile ad-hoc networks because of resource constraints. Despite making such sensor networks possible, the broadcasting nature of the sensors presents a number of security threats when deployed for certain applications like military, surveillances etc .The problem of security is due to the wireless nature of the sensor networks and constrained nature of resources on the wireless sensor nodes, which means that security architectures used for traditional wireless networks are not viable. However, wireless MANET is particularly vulnerable due to its fundamental characteristics, such as open medium, dynamic topology, distributed cooperation, limited bandwidth and limited battery power. Generally, routing security in MANETs appears to be a problem that is not trivial to solve. It is observed that the routing attacks have severe impact on MANET than WSN. In this paper we discuss some routing attacks and challenges faced by WSNs and MANETs and also add some secure routing protocols.

IndexTerms - Wireless Sensor Networks (WSN), Mobile Ad-Hoc Networks(MANET), Routing Protocols, Threats and Security Attacks.

I. INTRODUCTION

A Mobile Ad Hoc Network (MANET) is a collection of mobile devices which over a shared wireless medium can communicate with each other without the use of a predefined infrastructure. The member nodes are responsible for the creation, operation and maintenance of the network. Each node in the MANET is equipped with a wireless transmitter and receiver, using which it communicates with the other nodes in its wireless vicinity. The nodes which are not in wireless vicinity, communicate with each other hop by hop following a set of rules (routing protocols) for the hopping sequence to be followed. In addition to freedom of mobility, a MANET can be constructed quickly at a low cost which makes MANET attractive for applications such as disaster relief, emergency operations, military service etc.Wireless Sensor Networks (WSNs) consist of small nodes with sensing, computation, and wireless communications capabilities. The properties of wireless nodes are limited energy capabilities and limited computation and memory capacity on a dynamically changing environment. There are four basic components of sensor network and they are 1) an assembly of distributed or localized sensors 2) an interconnection network 3) a point of information clustering 4) a set of computing resources at base station to handle data collection and analyzing . Due to their own nature a variety of attacks are possible in Wireless Networks. These security attacks can be classified according to different criteria, such as the domain of the attackers, or the techniques used in attacks[1]. These security attacks can be roughly classified by the following criteria: passive or active, internal or external, different protocol layer, stealthy or non-stealthy, cryptography or non cryptography related. In this paper we are discussing only Network Layer attacks in MANET and WSN.

The rest of the paper is organized as follows: Section II presents the idea why secure network is required. Presently known routing attacks are presented in Section III. Section IV provides the challenges faced by Sensor networks. Section V gives some idea about secure routing protocols. And finally Section VI summarizes the paper with the direction in which future research should be done.

II. MOTIVATION

As sensor networks can operate in an ad-hoc manner the security goals cover both those of the traditional networks and goals suited to the unique constraints of ad-hoc sensor networks. The security goals are classified as primary and secondary [2]. The primary goals are known as standard security goals such as Confidentiality, Integrity, Authentication and Availability (CIAA). The secondary goals are Data Freshness, Self- Organization, Time Synchronization and Secure Localization.

A. *Data Confidentiality*- Confidentiality is the ability to conceal messages from a passive attacker so that any message communicated via the sensor network remains confidential. In many applications (e.g. key distribution) nodes communicate highly sensitive data. The standard approach for keeping sensitive data secret is to encrypt the data with a secret key that only intended receivers possess, hence achieving confidentiality[2]. Since public-key cryptography is too expensive to be used in the resource constrained sensor networks, most of the proposed protocols use symmetric key encryption methods.

B. *Data Authentication*- Authentication ensures the reliability of the message by identifying its origin. Attacks in sensor networks do not just involve the alteration of packets; adversaries can also inject additional false packets. Data authentication verifies the identity of the senders and receivers. Data authentication is achieved through symmetric or asymmetric mechanisms where sending and receiving nodes share secret keys.

***C. Data Integration*-** Data integrity ensures the receiver that the received data is not altered in transit by an adversary that refers to the ability to confirm that a message has not been tampered with, altered or changed.

***D. Data Availability*-** Availability determines whether a node has the ability to use the resources and whether the network is available for the messages to communicate.

***E. Data Freshness*-** Data freshness implies that the data is recent, and it ensures that an adversary has not replayed old messages [3]. A common defense is to include a monotonically increasing counter with every message and reject messages with old counter values.

F. *Self-Organization*- A wireless sensor network is a typically an ad hoc network, which requires every sensor node be independent and flexible enough to be self-organizing and self-healing according to different situations.

***G. Time Synchronization*-** Most sensor network applications rely on some form of time synchronization. Furthermore, sensors may wish to compute the end-to-end delay of a packet as it travels between two pair-wise sensors.

H. *Secure Localization*- The utility of a sensor network will rely on its ability to accurately and automatically locate each sensor in the network. A sensor network designed to locate faults will need accurate location information in order to pinpoint the location of a fault [3].

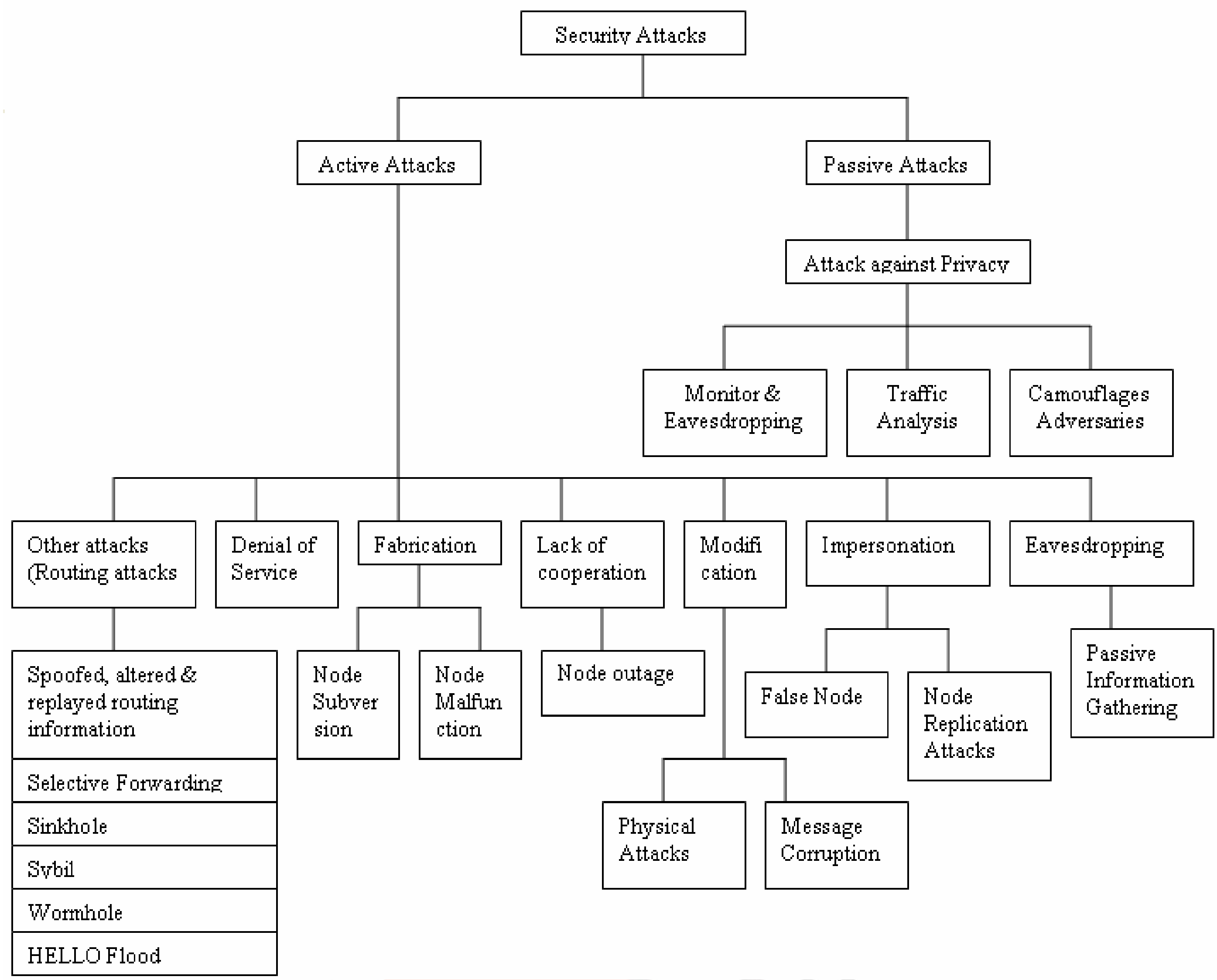
III. DIFFERENT ATTACKS IN MANET AND WSN

A. Attacks Classifications on Wireless Network: Security attacks are classified as passive and active attacks: Broadcast nature of the data transmission causes Wireless networks vulnerable to security attacks. Nodes are often placed in a hostile environment where they are not physically protected which causes the additional vulnerability.

***Passive Attacks*:** In passive attacks the attacker does not send any message, but just listens to the channel. Passive attacks are non disruptive but are information seeking, which may be critical in the operation of a protocol [4]. Adversaries need not be physically present to maintain surveillance; they can gather information at low-risk in anonymous manner.

A passive attacker listens to the channel and packets containing secret information (e.g., IP addresses, location of nodes, etc.) may be stolen, which violates confidentiality paradigm. In a wireless environment it is normally impossible to detect this kind of attack, as it does not produce any new traffic in the network.

***Active Attacks*:** Active attacks may either be directed to disrupt the normal operation of a specific node or target the operation of the whole network. The action of an active attacker includes injecting packets to invalid destinations into the network, deleting packets, modifying the contents of packets, and impersonating other nodes which violates availability, integrity, authentication, and non-repudiation paradigm. Contrary to the passive attacks, active attacks can be detected and eventually avoided by the legal nodes that participate in an ad hoc network.



INTERNAL AND EXTERNAL ATTACKS:

Internal and external attacks: According to the domain of the attacks these attacks are classified, external attacks are done by nodes that not belongs to domain of the network. Internal attacks are from compromised nodes, which are actually part of the network. Internal attacks are more severe than external attacks.

B. Attacks in WSN

Spoofing: The most direct attack against a routing protocol is to target the routing information exchanged between nodes [5]. By spoofing, altering, or replaying routing information,adversaries may be able to create routing loops, attract network traffic, extend or shorten source routes, generate false error messages, partition the network, increase end-to-end latency, etc. An unprotected ad hoc routing is vulnerable to these types of attacks.

Selective Forwarding: Multi hop networks are based on the idea that participating nodes will faithfully forward receive messages . In a selective forwarding attack , malicious nodes may refuse to forward certain messages and simply drop them, ensuring that they are not propagated any further in the network. Selective forwarding attacks are typically most effective when the attacker is explicitly included on the path of a data flow [5].

Sinkhole: Attracting traffic to a specific node in called sinkhole attack. In this attack, the adversary's goal is to attract nearly all the traffic from a particular area through a compromised node. Sinkhole attacks typically work by making a compromised node look especially attractive to surrounding nodes with respect to the routing algorithm [5].

Sybil: In a Sybil attack, a single node presents multiple identities to other nodes in the network. The Sybil attack can significantly reduce the effectiveness of fault-tolerant schemes and routes believed to be using disjoint nodes could in actuality be using a single adversary presenting multiple identities [5]. Sybil attacks also pose a significant threat to geographic routing protocols .

Wormhole: An adversary tunnels messages received in one part of the network over a low latency link and replays them in a different part. The simplest instance of this attack is a single node situated between two other nodes forwarding messages between the two of them [6].

Hello flood: An attacker sends or replays a routing protocol's HELLO packets from one node to another with more energy. This attack uses HELLO packets as a weapon to convince the sensors in WSN. In this type of attack an attacker with a high radio transmission range and processing power sends HELLO packets to a number of sensor nodes that are isolated in a large area within a network . The sensors are thus influenced that the adversary is their neighbor. As a result, while sending the information to the base station, the victim nodes try to go through the attacker as they know that it is their neighbor and are ultimately spoofed by the attacker [6].

C. MANET Attacks

Flooding - The aim of the flooding attack is to exhaust the network resources, such as bandwidth and to consume a node's resources, such as computational and battery power or to disrupt the routing operation to cause severe degradation in network performance [7].

Blackhole - In a blackhole attack, a malicious node sends fake routing information, claiming that it has an optimum route towards destination and causes other good nodes to route data packets through the malicious one.

Link Withholding - A malicious node ignores the requirement to advertise the link of specific nodes or a group of nodes, which can result in link loss to these nodes. This type of attack is particularly occurring in the OLSR protocol.

Link Spoofing - A malicious node advertises fake links with non-neighbors to disrupt routing operations. For example, in the OLSR protocol, an attacker can advertise a fake link with a target's two-hop neighbors [7]. This causes the target node to select the malicious node to be its Multi Point Relay (MPR). As an MPR node, a malicious node can then modify or drop the routing traffic or perform other types of DoS attacks.

***Replay* -** In a replay attack , a node records another node's valid control messages and resends them later. This causes other nodes to record their routing table with stale routes. Replay attack can be misused to impersonate a specific node or to disturb the routing operation in a MANET[8].

Wormhole- In this attack, a pair of colluding attackers record packets at one location and replay them at another location using a private high speed network. The seriousness of this attack is that it can be launched against all communications that provide authenticity and confidentiality [9].

Colluding Mis-Relay- In this attack, multiple attackers work in collusion to modify or drop routing packets to disrupt routing operation in a MANET. This attack is difficult to detect by using the conventional methods [10].

D. **New Types of Attack**:

Sleep deprivation torture attack: A malicious user may interact with a node in an otherwise legitimate way, but for no other purpose than to consume its battery energy. Battery life is the critical parameter for many portable devices, and many techniques are used to maximize it; in WSN, for example, nodes try to spend most of the time in a sleep mode in which they only listen for radio signals once in a while (the period can be set from a few seconds to several minutes). In this environment, power exhaustion attacks are a real threat, and are much more powerful than better known denial of service threats such as CPU exhaustion; once the battery runs out the attacker can stop and walk away, leaving the victim disabled. We call this technique the sleep deprivation torture attack [11].

IV. CHALLENGES FOR SENSOR NETWORKS

The nature of large, ad-hoc, wireless sensor networks presents significant challenges in designing security schemes. A wireless sensor network is a special network which has many constraint compared to a traditional computer network.

Wireless Medium- The wireless medium is inherently less secure because its broadcast nature makes eavesdropping simple. Any transmission can easily be intercepted, altered, or replayed by an adversary. The wireless medium allows an attacker to easily intercept valid packets and easily inject malicious ones [12].

Ad-Hoc Deployment- The ad-hoc nature of sensor networks means no structure can be statically defined. The network topology is always subject to changes due to node failure, addition, or mobility. Nodes may be deployed by airdrop, so nothing is known of the topology prior to deployment. Since nodes may fail or be replaced the network must support self-configuration. Security schemes must be able to operate within this dynamic environment.

Hostile Environment- The next challenging factor is the hostile environment in which sensor nodes function. Motes face the possibility of destruction or capture by attackers. Since nodes may be in a hostile environment, attackers can easily gain physical access to the devices. Attackers may capture a node, physically disassemble it, and extract from it valuable information like cryptographic keys [13]. The hostile environment poses a serious challenge for researchers.

Resource Scarcity- The hardware constraints necessitate extremely efficient security algorithms in terms of bandwidth, computational complexity, and memory. This is no trivial task. Energy is the most precious resource for sensor networks. Communication is especially expensive in terms of power.

Immense Scale- Security mechanisms must be scalable to very large networks while maintaining high computation and communication efficiency.

Unreliable Communication- Certainly, unreliable communication is another threat to sensor security. The security of the network relies heavily on a defined protocol, which in turn depends on communication [13].

Unattended Operation- Depending on the function of the particular sensor network, the sensor nodes may be left unattended for long periods of time.

Power Limitation – Sensor nodes are run by battery power that limited energy causes problem during data transmission in long distance, that's why multi-hop transmission is used.

V. SECURE ROUTING PROTOCOL

A. *ARIADNE*- A secure on-demand ad hoc network routing protocol, based on DSR, basic operations are Route Discovery and Route maintenance [14]. Ariadne prevents attackers or compromised nodes from tampering with uncompromised routes consisting of uncompromised nodes, and also prevents many types of Denial-of-Service attacks.

In addition, Ariadne is efficient, using only highly efficient symmetric cryptographic primitives. Ariadne can authenticate routing messages using one of three schemes: shared secret keys between all pairs of nodes, shared secret keys between communicating nodes combined with broadcast authentication, or digital signatures.

B. *Secure AODV* - SAODV is a security extension of the AODV protocol, based on public key cryptography. SAODV routing messages (RREQs, RREPs, and RERRs) are digitally signed to guarantee their integrity and authenticity [15].

A node that generates a routing message signs it with its private key, and the nodes that receive this message verify the signature using the sender's public key.

In its basic form, this makes it impossible for intermediate nodes to reply to RREQs if they have a route towards the destination, because the RREP message must be signed by the destination node.To preserve the collaboration mechanism of AODV, SAODV includes a kind of delegation feature that allows intermediate nodes to reply to RREQ messages. This is called the double signature.

When a node A generates a RREQ message, in addition to the regular signature, it can include a second signature, which is computed on a fictitious RREP message towards A itself. Intermediate nodes can store this second signature in their routing table, along with other routing information related to node A. If one of these nodes then receives a RREQ towards node A, it can reply on behalf of A with a RREP message, similarly to what happens with regular AODV.

SAODV requires heavyweight asymmetric cryptographic operations, every time a node generates a routing message, it must generate a signature, and every time it receives a routing message (also as an intermediate node), it must verify a signature.

SAODV requires heavyweight asymmetric cryptographic operations, every time a node generates a routing message, it must generate a signature, and every time it receives a routing message (also as an intermediate node), it must verify a signature.

This gets worse when the double signature mechanism is used, because this may require the generation or verification of two signatures for a single message [16].

C. *Secure Efficient Ad hoc Distance vector routing protocol* (SEAD) - A secure ad hoc network routing protocol based on the design of the Destination-Sequenced Distance-Vector routing protocol (DSDV). It's differ from DSDV in that SEAD do not use an average weighted settling time in sending triggered updates.

To reduce the number of redundant triggered updates, each node in DSDV tracks, for each destination, the average time between when the node receives the *first* update for some new sequence number for that destination, and when it receives the *best* update for that sequence number for it.

When deciding to send a triggered update, each DSDV node delays any triggered update for a destination for this average weighted settling time, for that sequence number. SEAD does not use such a delay, in order to prevent attacks from nodes that might maliciously not use the delay.

Since a node selects the first route it receives with highest sequence number and lowest metric, an attacker could otherwise attempt to cause more traffic to be routed through it, by avoiding the delay in its own triggered updates.

In addition, unlike DSDV, when a node detects that its next-hop link to some destination is broken, the node does not increment the sequence number for that destination in its routing table when it sets the metric in that entry to infinity.

SEAD did not include a mechanism for authenticating these larger sequence numbers. Instead, the node flags its routing table entry for this destination to not accept any new updates for this same sequence number [17].

D. *Service Location Protocol (SLP)* - SLP contains a public-key cryptography based security mechanism that allows signing of service announcements. In practice it is rarely used.

The public keys of every service provider must be installed on every node. This requirement defeats the original purpose of SLP, being able to locate services without prior configuration. Protecting only the services is not enough.

Service URLs contain host names or IP addresses, and in a local network it is almost impossible to prevent IP or DNS spoofing. Thus only guaranteeing the authenticity of the URL is not enough if any device can respond to the address.

As addresses can be spoofed, the authenticity of the device must be proven at a different level. Doing it additionally in SLP does not provide much additional security [18].

E. *Secure Link State Protocol (SLSP)* - The Secure Link State Protocol (SLSP) for mobile ad hoc networks is responsible for securing the discovery and distribution of link state information. The scope of SLSP may range from a secure neighborhood discovery to a network-wide secure link state protocol. SLSP nodes disseminate their link state updates and maintain topological information for the subset of network nodes within their Zone [19].

F. *Secure Routing Protocol (SRP)* – SRP makes security association between two communicating nodes Source and Destination. Route request packets propagate to the destination and route replies are returned to source over the reversed route. Route error messages are generated by nodes lie on the route reported as broken. To provide functionality, SRP explicitly interact with Network Layer. It also provides a novel way of query identification which protects query propagation and end nodes from DoS attacks [20].

G. *Authenticated Routing for Ad hoc Networks (ARAN)* - This secure routing protocol detects and protects against malicious actions by third parties and peers in one particular ad hoc environment.

ARAN consists of a preliminary certification process followed by a route instantiation process that guarantees end-to-end authentication.

The protocol is simple compared to most non-secured ad hoc routing protocols, and does not include routing optimizations. It should be noted that these optimizations are the chief cause of most routing attacks.

Route discovery in ARAN is accomplished by a broadcast route discovery messages from a source node that replied to by the destination node.

The routing messages are authenticated end-to-end and only authorized nodes participate at each hop between source and destination [21].

VI. *CONCLUSION AND FUTURE WORK*

Wireless Network is resource constrained. Therefore; existing security schemes for wired networks cannot be applied directly to wireless, which makes them much more vulnerable to security attacks.

Future research should be focused on exploring, as well as preventing all possible attacks to make wireless network a secure and reliable place.

REFERENCES

[1] Ray Hunt, Network Security: “The Principles of Threats, Attacks and Intrusions, part1 and part 2 , “ APRICOT, 2004.

[2] Ian F. Akykildiz, Weilian Su, Yogesh Sankarasubramaniam, and Erdal Cayirci,”A Survey on Sensor Networks”, IEEE Communication Magazine, year 2002.

[3] Y. Wang, G. Attebury, and B. Ramamurthy, “A Survey of Security Issues in Wireless Sensor Networks” ,IEEECommun. Surveys Tutorials,vol.8, pp. 2–23, year 2006.

[4] Undercoffer, J., Avancha, S., Joshi, A. and Pinkston, J, ”Security for sensor networks”. In Proceedings of the CADIP Research Symposium, University of Maryland, Baltimore County,USA, year 2002 http://www.cs.sfu.ca/~angiez/personal/paper/sensor- ids.pdf

[5] Chris Karlof, David Wagner, “Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures”, AdHoc Networks (elsevier), Page: 299-302, year 2003.

[6] Zia, T.; Zomaya, A.,”Security Issues in Wireless SensorNetworks”,Systems and Networks Communications (ICSNC) Page(s):40 – 40, year 2006.

[7] P. Yi et al., “A New Routing Attack in Mobile Ad Hoc Networks”, Int’l. J. Info. Tech., vol. 11, no. 2 , 2005.

[8] C. Adjih, D. Raffo, and P. Muhlethaler, “Attacks Against OLSR: Distributed Key Management for Security”, 2nd OLSR Interop/Wksp., Palaiseau, France, July 28–29, 2005.

[9] Yin-Chun Hu, Adrian Perrig, and David B. Johnson, “Wormhole Attacks in Wireless Networks”, IEEE JSAC, vol. 24, no. 2, Feb , 2006.

[10] B. Kannhavong et al., ”A Collusion Attack Against OLSR-Based Mobile Ad Hoc Networks”, IEEE GLOBECOM ’06.

[11] Frank Stajano, Ross Anderson ,“ The Resurrecting Duckling ,Security Issues for Ad-hoc Wireless Networks “ Security Protocols, 7th International Workshop , Proceedings, LectureNotes in Computer Science, 1999.Springer-Verlag Berlin Heidelberg 1999 .

[12] John Paul Walters, Zhengqiang Liang, Weisong Shi, Vipin Chaudhary, “Wireless Sensor Network Security: A Survey”, Security in Distributed, Grid and Pervasive Computing Yang Xiao (Eds), Page3-5, 10-15, year 2006.

[13] Tahir Naeem, Kok-Keong Loo, Common Security Issues and Challenges in Wireless Sensor Networks and IEEE 802.11 Wireless Mesh Networks, International Journal of Digital Content Technology and its Applications, Page 89-90 Volume 3, Number 1, year 2009.

[14] Yih-Chun Hu, Adrian Perrig , David B. Johnson “Ariadne: A Secure On- Demand Routing Protocol for Ad Hoc Networks ,” Wireless Networks 11, 21–38, 2005 Springer Science & Business Media, Inc.Manufactured in The Netherlands.

[15] Davide Cerri and Alessandro Ghioni, “Securing AODV: The A-SAODV Secure Routing Prototype , “ IEEE Communications Magazine , February 2008 .

[16] M. Guerrero Zapata and N. Asokan, “Securing Ad hoc Routing Protocols,” Proc. 1st ACM Wksp. Wireless Sec., Sept. 2002, pp. 1–10 .

[17] Yih-Chun Hu, David B Johnson, Adrian Perrig “ SEAD: secure efficient distance vector routing for mobile wireless ad hoc networks ,“ 2003 Ad Hoc Networks ,Springer .

[18] James Kempf, Robert St. Pierre, Pete St. Pierre, “ Service Location Protocol for Enterprise Networks: Implementing and Deploying a Dynamic Service Finder ,” John Wiley & Sons, ISBN 0-471-31587-7 .

[19]P. Papadimitratos , Zygmunt J. Haas , “Secure Link State Routing for Mobile Ad Hoc Networks ,“ Applications and the Internet Workshops, 2003. Proceedings , IEEE , pp- 379 - 383.

[20]P.Papadimitratos and Z.J.Haas, “Secure Routing for Mobile Ad hoc Networks,” Proceedings of IEEE Workshop on Security and Assurance in Ad hoc Networks, IEEE Press, pp. 27-31, 2003.

[21]K.Sanzgiri, B.Dahill, B.N.Levine, C.Shields and E.M. Royer, “A Secure Routing Protocol for Ad hoc Networks”, Proceedings of 10th IEEE International Conference on Network Protocols (ICNP’02), IEEE Press, pp. 78-87, 2002 .