ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

Volume 3, Special Issue 3, March 2014

2014 International Conference on Innovations in Engineering and Technology (ICIET'14)
On 21st & 22nd March Organized by

K.L.N. College of Engineering , Madurai, Tamil Nadu, India

A Valuable Secure Protocol to Prevent Vampire Attacks In Wireless Ad Hoc Sensor Networks

K.Vanitha,V.Dhivya

PG scholar, Department of CSE, K.Ramakrishnan College of Technology, Samayapuram, Tiruchirapalli, India

Assistant Professor, Department of CSE, K.Ramakrishnan College of Technology, Samayapuram, Tiruchirapalli, India

Abstract— An ad hoc network is a group of wireless nodes, in which each node can communicate over multihop paths to any other node without the help of any preexisting infrastructure such as base station or access points. Owing to these feature ad hoc low power wireless networks are capable of sensory and pervasive computing which forms the wireless ad hoc sensor network. Ad hoc require no centralized administration so the network infrastructure can be formed quickly and inexpensive set up is needed. Ad hoc networks are being used in military operation, emergency disaster relief and community networking. An important security issue that has been identified in these networks is resource depletion attack at routing layer protocol. These attacks drain nodes battery power completely, so that the network is permanently disabled. Hence these attacks are termed as vampire attacks. Even as there exist many secure routing protocols, they are unable to protect the network from vampire attacks. So as an attempt to eliminate vampire attacks, three primary contributions has been introduced. i. Evaluation of the vulnerabilities of existing protocols. ii. Quantization of performance of various protocols in the existence of solitary vampire. iii. Modification of existing protocol to deplete vampire attacks.

Keywords—Ad hoc sensor network, routing, security, denial of service, vampire attack, PLGP

I. INTRODUCTION

A network is composed of nodes each of which has computing power and can transmit and receive message over communication links, wireless or cabled. In Wireless networks each node use radio signal to communicate with other nodes. A wireless ad hoc sensor network consists of a number of sensors spread across a geographical area. Each sensor has wireless communication capability and some level of intelligence for signal processing and networking of the data. The basic characteristic of ad-hoc sensor network is the communication among nodes of network without any pre-existing infrastructure. Wireless Ad hoc Sensor Network have become very essential in communication environment. Due to distributed nature of these networks and their deployment in remote areas, these networks are Susceptible to several security threats that can adversely affect their proper functioning. Ad hoc sensor network guarantees pervasive computing, instantly deployable communication for military and continuous connectivity, for creating a new application in future. Resource constrains is one of the main characteristic of a Wireless sensor networks Simplicity in WSN with resource constrained nodes makes them very much vulnerable to denial of service [1], attacks on routing infrastructure, and reduction of quality attacks.

Routing techniques are required for sending data between sensor nodes and base station for communication. There are many ways to classify the routing protocols. Almost all of the routing protocols can be classified as data-centric, hierarchical and location based according to the network structure. In data-centric routing all nodes are typically assigned equal roles or functionality. In hierarchical-based routing however, nodes will play different role in the network. In location-based routing sensor node's positions are exploited to route data in the network. 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. Although this problem is not unique to sensor networks, traditional solutions must be adapted to efficiently execute on sensor networks. Developing energy-efficient routing protocol on wireless sensor networks is one of the important challenges. Therefore, a key area of WSN research is to

develop a routing protocol that consumes low energy. Unfortunately, current routing protocols suffer from many security vulnerabilities. Already many solutions have been proposed to defend attack that live for short duration on the network [3][4]. But these solutions do not defend permanent resource depletion attack. The battery power consumption attacks at routing layer protocol to completely disable networks, by depleting node's battery power and it is defined as vampire attacks. These attacks never flood the network with large amount of data instead it drains node's life by delaying the packets. Protocols such as SEAD[6], Ariadne[7], SAODV[13]are securely designed but do prevent the vampire attacks Existing security scheme are limited to other layers such as medium access control or application layers but not to the routing layer to secure vampire attacks[5]. In section 2 energy draining attacks in source routing protocol is reviewed. In section 3 evaluation of energy draining attacks on stateless and stateful routing protocol. In section 4 secure routing protocols against vampire attacks are discussed. Section 5 presents a simulation based performance comparison of existing and proposed protocol. In section 6 presents the conclusion.

II. Overview

Energy/Power Consumption of the sensing device should be minimized since their limited energy resource determines their lifetime. Communication is especially expensive in terms of power. Security mechanisms must give special effort to be communication efficient in order to be energy efficient. Providing security over such a network is equally challenging. Security mechanisms must be scalable to very large networks while maintaining high computation and communication efficiency. Depending on the function of the particular sensor network, the sensor nodes may be left unattended for long periods of time. Vampire attack has influenced the protocols like link state, distance vector, source routing, beacon routing and sensor routing .

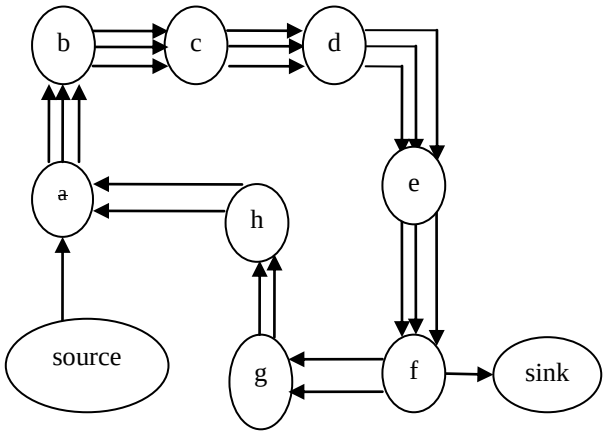

Fig. 2. 1 An honest node would exit the loop immediately from node, but a malicious packet makes its way around the loop twice more before exiting.

In source routing protocol a malicious source can construct a route that leads to (a) carousel attack and (b) stretch attack. In carousel attack an adversary forms a loop for routing packets as shown in Fig.1.In stretch attack an adversary construct artificially long routes as shown in Fig.2.

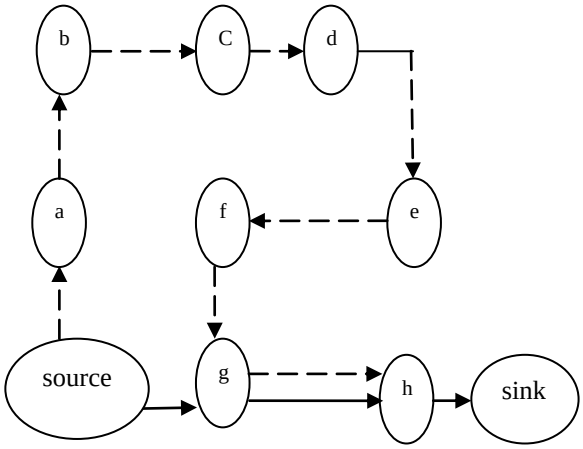

Fig. 2.2.Honest node with thick line and malicious node with thin lines.

Many methods are analyzed to limit the damage caused by vampire attack. The first mechanism considered to protect these attacks is loose source routing, in which any forwarding node can reroute the packet if it knows a shortest path to the destinations. In second attempt to modify the protocol (PLGP) from [12] to guarantee that a packet makes progress through the network. This is called as No- backtracking property, because it holds if and only if a packet is moving strictly closer to destination with every hop. No-backtracking is not satisfied in case of non source routing protocol. To preserve no-backtracking property add a verifiable path history to the packet. Elliptic curve cryptography technique is used to verify the packet comes originate from authorize node.

III. Energy Drainiing Attacks on Stateless And Stateful Protocol

In the DSR[9] source node specifies the entire route in the packet header to a destination, so intermediate node's do not make independent forwarding decisions, instead of a route specified by the source. To forward a message, the intermediate node finds itself in the route and transmits the message to the next hop. The fardel is on the source to ensure that the route is valid at the time of sending, and that every node in the route is a physical neighbor of the previous route hop. Both the carousel and stretch attacks are evaluated in a randomly generated 30-node topology. It causes delay as well as increase communication overhead and energy consumption in resource limited networks .The effect of denial or degradation of service on battery life and other finite node resources has not generally been a considered securely.

1) Carousel attack: In this attack, a malicious node forward a packet with a route included a chain of loops, such that the packets traverse several times in the same route. This strategy can be used to increase the route length beyond the number of nodes in the network An

example of this type of route is in Fig.3the thick path shows the honest path and thin shows the malicious path.

2) Stretch attack: Another attack in the same layer is the stretch attack, where a malicious node constructs falsely long source routes, causing packets to traverse a longer than optimal number of nodes. In this example given below honest path shown with thick lines and adversary or malicious path with thin lines. The honest path is very less distant but the malicious path is very long to make more energy consumption. Per-node energy usage under both attacks is shown in Fig.5. As expected, the carousel attack causes excessive energy usage for a few nodes, since only nodes along a shorter path are affected.

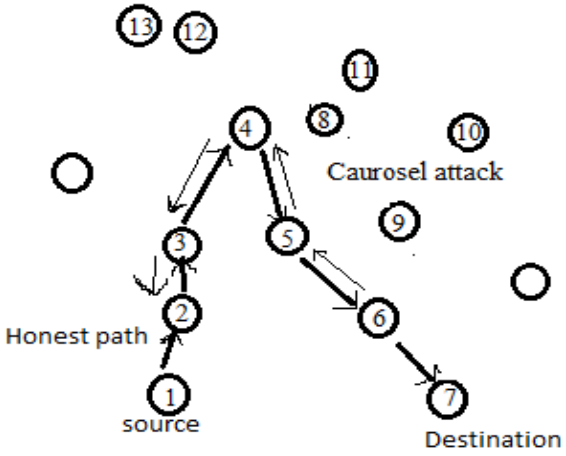

Fig. 3.1 shows the caurosel attack same node appears in the route many times.

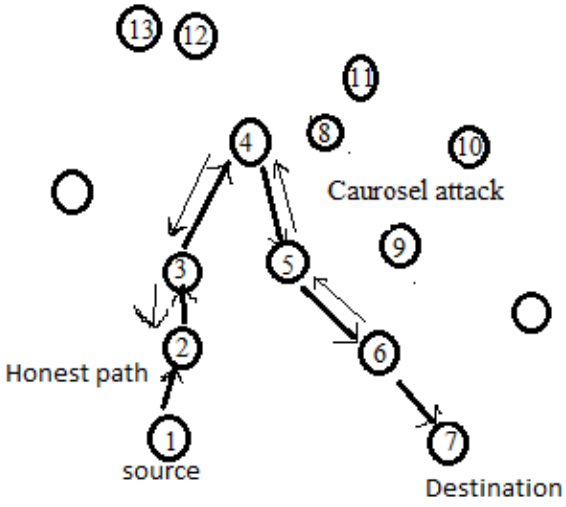

Fig. 3.2 Shows Stretch attack with two different paths from source to destination.(4-9-10-11-12-8-9—long route)

In contrast, the stretch attack shows more uniform energy consumption for all nodes in the network, since it lengthens the route, causing more nodes to process the packet. While both attacks drastically network-wide energy usage, individual nodes are also noticeably affected, with some losing almost 10 percent of their total energy reserve per message.

Two important classes of stateful protocols are link-state and distance-vector. In link-state protocols, such as OLSR [2], nodes keep a record of the up-or-down state of links in the network, and flood routing updates every time a link goes down or a new link is enabled. Distance vector protocols like DSDV [11] keep track of the next hop to every destination, indexed by a route cost metric, e.g., the number of hops. In this scheme, only routing updates that change the cost of a given route need to be propagated. Routes in link-state and distance-vector networks are built dynamically from many independent forwarding decisions, so adversaries have limited power to affect packet forwarding, making these protocols immune to carousel and stretch attacks.

In GPSR, a packet may encounter a dead end, which is a localized space of minimal physical distance to the target, but without the target actually being reachable. The packet must then be diverted until a path to the target is available. In BVR, packets are routed toward the beacon closest to the target node, and then move away from the beacon to reach the target. Each node makes independent forwarding decisions, and thus a Vampire is limited in the distance it can divert the packet. These protocols also fall victim to directional antenna attacks in the same way as link-state and distance-vector protocols above, leading to energy usage increase factor of $O(d)$ per message, where d is the network diameter. Moreover, GPSR does not take path length into account when routing around local obstructions, and so malicious misrouting may cause up to a factor of $O(c)$ energy loss, where c is the circumference of the obstruction, in hops.

IV. Valuable Secure Protocol Against Vampire Attacks

This section shows that the modification of clean slate secure sensor routing protocol [12] is provable security against vampire attack. The real version of this protocol is designed for security but it is vulnerable to vampire attacks. A new valuable secure protocol(VSP) is proposed to prevent vampire attacks consists of following phases.

A. Network Configuring Phase

A network describes a collection of nodes and the links between them. The neighbor group formation process is done by each and every node in the network. This is the process of calculate the neighbor node value and find surrounding node. The neighbor list is maintained by all of nodes in the network. This process constructs a neighbour relationship tree and group membership that will used for addressing and routing. At the end of this process, each node learns every other node's virtual address, public key, and certificate, since every group members knows the identities of all other group members and the network converges to a single group Each and every node has initial energy value by it creation time.

Every new nodes need to be authenticated before being allowed to join the WSN.

B. Key Management

This key management process is used for cryptography application during data transfer. Nodes generate a key to communicate with nodes in a group. Generated Key is established to all other nodes in a group. Every packet is encrypted and forwarded along the route. The cryptography technique used to protect the node and data from different kind of attacks. Elliptic curve cryptography (ECC) is an approach to public-key cryptography based on the algebraic structure of elliptic curves over finite fields. Compared with the other cryptography, ECC offers a better performance because it can achieve the same security with a smaller key size. It will minimize the number of calculation as well as save the time for nodes. communication takes place independently by each node in a group.

C. Communication Phase

Communication across a network is performed by secure routing protocol is PLGP In PLGP node cannot able to determine the route to promote the packet. This makes malicious nodes to redirect the packets to any part of the network even if that distance is logically further away from the destination. The same data packets transmitting through the same node repeatedly to deplete the batteries quickly and leads to network death because of vampire . No-backtracking property is introduced to overcome this problem. It implies that for each packet in the protocol execution trace, the number of in-between honest nodes traversed by the packet between source and target is self-determining action of malicious nodes. The malicious node cannot perform carousel or stretch attack. Intelligent adversary may still influence packet progress. To prevent this situation by independently checking on packet movement to the destination. In non source routing protocol packet routes are controlled by neighbour relationship and routing tree. Every node holds an identical copy of the address tree, and can verify the next logical hop. But this is not sufficient for backtracking.

Function Secure packet forward(p)

```
s -- get source address (p);
a – attestation (p);
if ( source sig is not verified (p) ) or
 (empty (a) and not is neighbour (s)) then drop(p);
for each node in a a do
   prevnode – node;
if ( not are neighbours (node , prevnode) ) or
( not making_progress (prevnode, node)) then - drop(p);
 c – nearest next node (s);
 p' – add (p);
 if is_neighbor ( c ) then send ( p' ,c );
else forward ( p' , next hop to non neighbor ( c ) );
```

To protect no-backtracking, add a certifiable path history to every PLGP packet. The resulting protocol, PLGP with attestations (PLGPa) uses this packet history together with PLGP's tree routing structure so every node can securely verify progress, preventing any malicious influence on the path taken by any packet which traverses influence on the path taken by any packet which traverses at least one honest node. Every node in a network maintain a neighbor list . The resulting protocol, PLGP with attestations (PLGPa) uses this packet history together with PLGP's tree routing structure so every node can securely verify progress, preventing any malicious influence on the path taken by any packet which traverses at least one honest node. Whenever node n forwards packet p, by attaching a signature which cannot be modified by any node. These signatures form a chain attached to every packet, allowing any node receiving it to validate its path. Every forwarding node validate the attestation chain to ensure that the packet has never traveled away from its destination in the logical address space . Fig 4.1 shows the data flow diagram of proposed protocol.

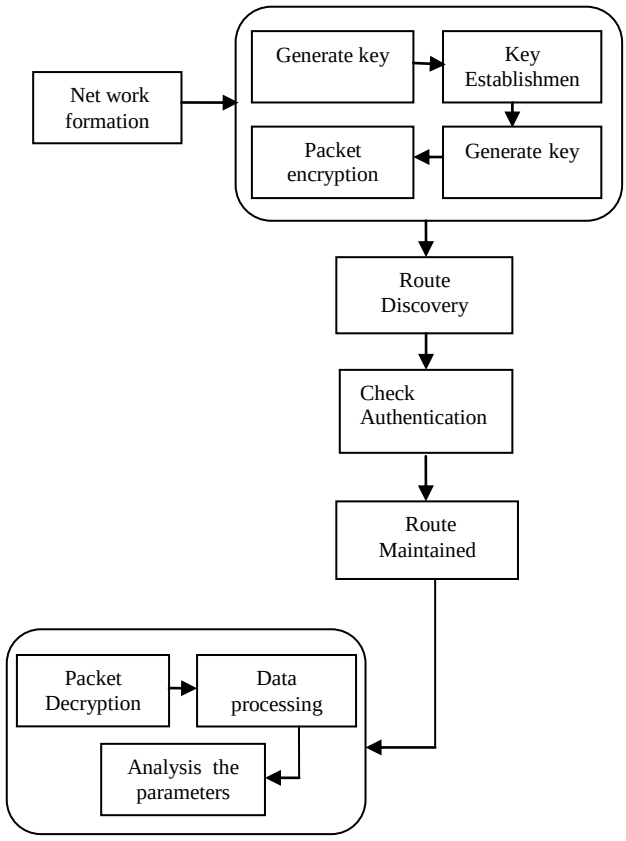

Fig.4.1 Flow Diagram of Secure Protocol

V.PERFORMANCE EVALUATION

A. Simulation set up

We conduct a series of simulations to evaluate the performance of PLGP, and compare with PLGPA with ecc. We launch the simulation on NS2. The Distributed Coordination Function (DCF) of the IEEE 802.11 protocol is used as the MAC layer protocol. The radio channel model follows a Lucent's WaveLAN with a bit rate of 2 Mbps, and the transmission range is 250 meters. We consider constant bit rate (CBR) data traffic and randomly choose different source-destination connections.

Every source sends four CBR packets whose size is 512 bytes per second. The mobility model is based on the random waypoint model in a field of 1000 m X 1000 m. ..

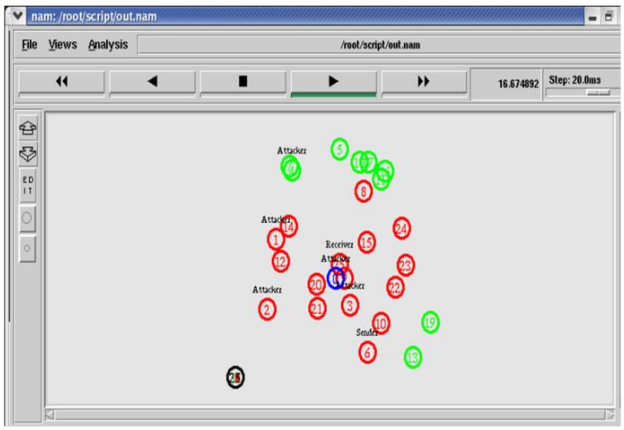

Fig.5.1 shows the attacks in nam output

A Valuable secure protocol is proposed to prevent the damage caused by vampire and reducing the energy usage in a network Evaluate the performance of existing and proposed protocol has been done using ns2 simulator. Fig 6 shows vampire attacks in a randomly generated topology of 30 nodes .Fig 7 shows prevention of vampire attack using PLGPa with ECC model.

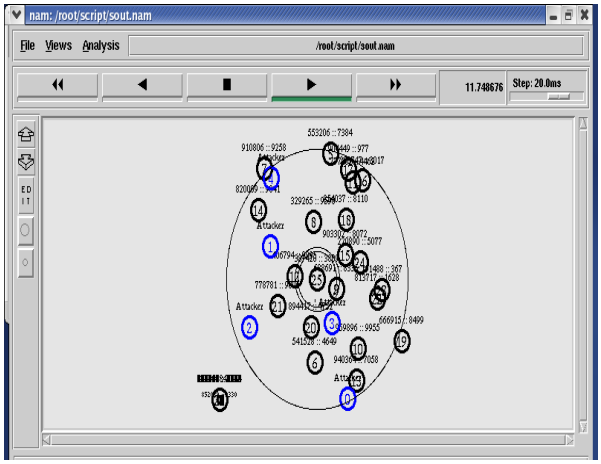

Fig.5.2 shows implementation PLGPa with ECC

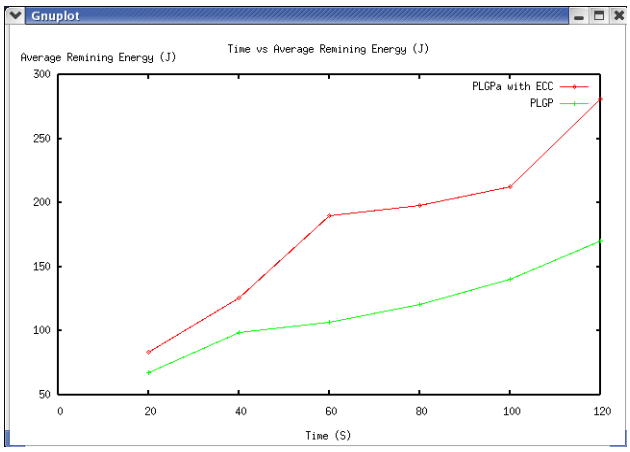

Fig. 5.3 average remaining energy

Simulation results shows that PLGPa with ECC reduces the network energy expenditure compare to existing protocol. In Fig 8 each node generate public and private key pair for secure communication the average remaining energy available in a network is more while using PLGPa with ECC

VI. Conclusion

A new class of energy draining attacks that use routing protocols to permanently halt ad hoc wireless sensor networks by depleting nodes' battery power. Vulnerabilities exposed in existing protocols are evaluated. Performance of existing protocols is quantified using small number of adversaries in a randomly generated 30 node topology. Simulation results show the network energy expenditure. Secure routing protocol PLGPawith ECC is proposed to prevent vampire attacks by verifying that packets make progress towards their destination.

REFERENCES

[1] I. Aad, J.-P. Hubaux, and E.W. Knightly, "Denial of Service Resilienc in Ad Hoc Networks," Proc. ACM MobiCom, 2004.

[2] H. Clausen and P. Jacquet, Optimized Link State Routing Protocol (OLSR), IETF RFC 3626, 2003.

[3] J. Deng, R. Han, and S. Mishra, "Defending against Path-Based DoS Attacks in Wireless Sensor Networks," Proc. ACM Workshop Security of Ad Hoc and Sensor Networks, 2005.

[4] J. Deng, R. Han, and S. Mishra, "INSENS: Intrusion-Tolerant Routing for Wireless Sensor Networks," Computer Comm., vol. 29, o. 2, pp. 216-230, 2006.

[5] Eugene Y.Vasserman , Nicholas Hopper, Vampire attack Draining life from wireless ad-hoc sensor networks. IEEE Transactions on Mobile Computing, Vol. 12, No. 2, February 2013

[6] Y.-C. Hu, D.B. Johnson, and A. Perrig, "SEAD: Secure Efficient Distance Vector Routing for Mobile Wireless Ad Hoc Networks," Proc. IEEE Workshop Mobile Computing Systems 2002.

[7] Y.-C. Hu, D.B. Johnson, and A. Perrig, "Ariadne: A Secure On- Demand Routing Protocol for Ad Hoc Networks," Proc. MobiCom, 2002

[8] Y.-C. Hu, D.B. Johnson, and A. Perrig, "Packet Leashes: A Defense against Wormhole Attacks in Wireless Ad Hoc Networks," Proc.IEEE INFOCOM, 2003

[9] D.B. Johnson, D.A. Maltz, and J. Broch, "DSR: The Dynamic Source Routing Protocol for Multihop Wireless Ad Hoc Networks"Ad Hoc Networking, Addison-Wesley, 2001.

[10] T.J. McNevin, J.-M. Park, and R. Marchany, "pTCP: A Client Puzzle Protocol for Defending Against Resource Exhaustion Denial of Service Attacks," Technical Report TR-ECE-04-10, Dept of Electrical and Computer Eng., Virginia Tech, 2004..

[11] C.E. Perkins and P. Bhagwat, "Highly Dynamic Destination-Sequenced Distance-Vector Routing (DSDV) for Mobile Computers," Proc. Conf. Comm. Architectures, Protocols and Applications,1994.

[12] B. Parno, M. Luk, E. Gaustad, and A. Perrig, "Secure Sensor Network Routing: A Clean-Slate Approach," CoNEXT: Proc. ACM CoNEXT Conf., 2006.

[13] M.G. Zapata and N. Asokan, "Securing Ad Hoc Routing Protocols," Proc. First ACM Workshop Wireless Security,2002