Volume 3, No. 3, May-June 2012

ISSN No. 0976-5697

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

Detecting and Preventing Wormhole Attacks in Wireless Sensor Networks using Secure Routing Algorithms

A.Thomas Paul Roy
Associate Professor, Computer Science and Engineering Department
PSNA College of Engineering and Technology
Dindigul, Tamil Nadu, India 624 622
pauli.dgl@gmail.com

Abstract: The resource constrained ad hoc wireless sensor network is versatile yet vulnerable to attacks. The communication infrastructure with less sensor networks may interact with the sensitive data in the hostile environment where the nodes may fail and new nodes may join the network, which may leads to the susceptibility to many kinds of security attacks. An adversary can eavesdrop on all the messages within the emission area, by operating in promiscuous mode. So, it is imperative that the protection of the network routing from the adversaries for the wireless ad hoc sensor network must be adopted for critical missions. A particularly devastating attack, predominant in today's world is the wormhole attack. In this paper, the wormhole attack made by the malicious attacker in sensor networks has been implemented and also the number of Guard nodes required has been decided and implemented. Functions of the guard nodes like local inter-node collaborative data fusion and decision fusion to detect, isolate and prevent any further attacks is to be implemented. Simulations have been performed under different scenarios and from the results of simulation we have observed that our scheme is capable of improving the security in resource constrained wireless sensor networks.

Keywords: Wireless Sensor Network, AODV, Wormhole

I. INTRODUCTION

The ad hoc wireless sensor networks is built, deployed, operated and maintained by the constituent wireless nodes in a highly hostile environment. Routing in ad hoc wireless sensor networks is an especially hard task to accomplish securely, robustly and efficiently. Reducing the vulnerability of sensor networks is a top priority. There are heavy restrictions in the sensor networks such as the low power devices, dynamic topology, variable capability links, energy constraints, power constraints, bandwidth constraints, inherent storage constraints, lack of post-deployment geographical configuration information constraints [1] and limited physical security.

Wormhole attack is one of the Denial-of-Service attacks effective on the network layer, that can affect network routing, data aggregation and location based wireless security. The wormhole attack may be launched by a single or a pair of collaborating nodes. In commonly found two ended wormhole, one end overhears the packets and forwards them through the tunnel to the other end, where the packets are replayed to local area.

In the paper, the various possible ways of detecting a particularly devastating termed the wormhole attack has been implemented and the wormhole attack prevention in the network layer is also implemented. The alien adversary nodes enter this dynamic reactive routing topology network during its route maintenance phase. The proposed mechanism to detect the malicious adversary node is based on the node density in the network and on the inter-node data and decision fusion local monitoring of these nodes to eliminate the attack. The proposed secured algorithm for routing protocol takes the sensor network limitation issues into consideration.

A. Wormhole Attacks:

In wormhole attack, an attacker can introduce two transceivers into a wireless network and connect them with a high quality, low-latency link. Wormhole attacks enable an attacker with limited resources since there is no cryptographic material to wreak havoc on wireless networks. The attacker can be internal attacker or external attacker or compromised internal attacker and can either passively eavesdrops into the network or actively inject packets into the network. There are four different modes in the wormhole attack: Packet Replay attack, Out-of-band attack, High Power Transmission attack and Protocol Deviation attack.

In the packet replay, an external or a compromised internal attacker records packet at one location of the network, tunnel them to another location of the network or to tunnel them to the same location at some other instant of time. In the out-of-band attack mode, the two colluding attackers attack with a long directional wireless link, giving an illusion to the nodes as its neighbor within its communication range. The attack requires specialized hardware capability to launch. In high power transmission attack mode, when a single malicious node gets a route request, it broadcasts the request at a high power level, a capability which the other nodes in the network do not posses.

II. LITERATURE SURVEY

The ad hoc wireless sensor networks operate on low resource constraints of power, battery life, and bandwidth in a highly hostile environment. All proposed solutions to thwart wormhole attack [2] [3] detect and prevent only few types of wormhole attack and are not survilent to all kinds of wormhole attacks. The success of the wormhole attack is its

strength of the attack independent of the cryptographic method. The solution based on the dependency of the cryptography [4][5] is vulnerable to wormhole replay attacks. This solution protects the routing from adversaries during the data-forwarding phase using the technique of One-Time Signature. There are two types of wormholes identified: one with malicious nodes revealing their identity and the other as the malicious nodes not revealing their identity.

The sensors are intended to be power limited and low-cost disposable devices, so the solution for the prevention of the attacks based on the antenna and the global positioning system are inadequate for wireless sensor networks [6]. To resolve the issue of topology based wormhole detection, in which the attacker uses a long directional antenna, the solution of the packet leashes [8] requires time synchronization, which is difficult to achieve in wireless sensor networks, because of the additional hardware requirements. The same solution fits for the replay attack on the lower MAC layer based on the physical proximity. The MAC Layer attacks and the solution of intrusion detection system of security features against the attacks by a Key Distribution Center in the routing protocol [8] [9].

The secured data forwarding schemes and the analysis of the secure data forwarding protocol that discusses the security in the data packets in the route maintenance phase are proposed in [10]. The authentication between the two legitimate neighboring nodes is secured with password protection with authenticated key exchange [7][10] for the security against the active intruders but fails to eliminate the passive intruders during the data exchange and is based on the transport layer security issues. The authentication between nodes can be provided by the localization of the certification process, public key infrastructure (PKI) distribution certification, and secured pair wise key distribution [10][11]. During the packet forwarding, nodes are categorized based on dynamic behavior [12]. Using which, misbehaved nodes will be avoided during transit. At this instant, packet forwarding between two-hop neighbors [13] has to be analyzed based on route reply packet. To check the validity of sender a unique key between the individual sensor node and the base station is required to be generated by suitable scheme. The survey analyses [14] that network layer data forwarding is highly viable to security breach and susceptible to design issues such as power efficiency, data centric & aggregation and location awareness.

The Byzantine attackers perform routing flawlessly but tell lies about routing information and thus failing to forward some routing packets correctly. In the Blackhole attack, an attacker suppresses or modifies packets originating from some nodes, while leaving the data from the other nodes unaffected, which limits the suspicion of its wrongdoing. Further surveys on the infrastructure less resource constrained network with limited physical security in a dynamic topology [15] list the wormhole, Sinkhole (Black hole) and Byzantine attacks as highly vulnerable and advanced attacks in the network layer in the wireless sensor ad hoc networks.

III. SYSTEM ARCHITECTURE

A. Introduction:

It provides an overview of the entire system architecture. This section describes all data, architectural, interface and component-level design for the software developed.

a. Modular Decomposition:

The modular decomposition of the entire software with its individual modular function is shown in figure 3.1

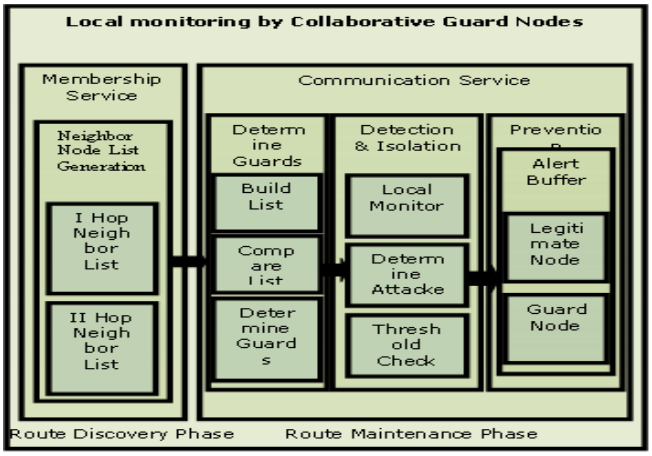

Figure 1 Modular Decomposition of the software

A description of the individual components for the architecture of the software developed "Guard Node based Collaborative Local Monitoring Prevention System Against Sophisticated Routing Attacks in Wireless Sensor Networks" is given in this section for the individual components of Topology Establishment, Attack Establishment and the Elimination Management.

B. Implementation Techniques:

a. Description for Topology Establishment:

This component serves to establish the network of mobile nodes in the environment of the sensor network. The nodes positioning in three-dimensional view is the basic implementation in this module, which is shown in figure 3.2. This section involves in the node positioning, node communication, control packet routing and the data packet routing.

b. Sub-Component 1: Node Positioning:

100-1000 nodes are deployed in the sensor network randomly that keeps changing for every 5000 ms. The first hop neighbor node must authenticate their existence within a time bound 5 ms and authenticated nodes are added up to Neighbor List Routing Table. If the sent node does not receive the authentication within the time bound then the nodes are not added to the Neighbor List Routing Table

c. Sub-Component 2: Node Communication:

AS-1: The malicious adversary will place nodes at arbitrary places in the sensor network.

AS-2: The adversary will not compromise the integrity and authenticity of the communication and any cryptographic quantity between the legitimate nodes remains secret.

DE-1: If r is the communication range of the sensor nodes in a circular area of communication. The area of the sensor networks is Πr^2 and the circumference is $2\Pi r$. The network field area under consideration Πr^2 must be large, and so the edge effects due to $2\Pi r$ will be negligible.

d. Sub-Component 3: Control Packet Routing:

The first hop neighbor node must authenticate to the received control packet from the sender node within a time bound 5 ms. If the authentication is not received within the time bound then the source sender node will resend the control packet. If the receiver node for 5 subsequent messages does not respond the authentication, then high priority is given to watch these nodes malicious act.

e. Sub-Component 4: Data Packet Routing:

After the control packet is received the neighbor node will send the data packet in the next consequent 1 ms. The received one hop neighbor node must authenticate to the received data/message packet within a time bound 5 ms. If the authentication is not received within the time bound then the source sender node will resend the data packet. If the receiver node for 5 subsequent messages does not respond the authentication, then high priority is given to watch these nodes malicious act.

C. Description for Attack Establishment:

This module establishes the attack in the created scenario of the mobile wireless sensor networks. The attacker enters sensor network topology and attacks the network as external attacker, internal attacker or a compromised internal attacker and causes malicious activities like provides illusion as the shortest path neighbor, drop data packets, performs Denial of Service, performs disruption in routing and contributes to faulty data. The attacker can be attack with the following modalities as in the Table 1.

Table 1 Vulnerabilities of the Wormhole Attack Modes

Mode Name	Attack	Attacker Model	Special Requirements
Packet Replay	External	Node Centric	High energy source
Packet Replay	Internal	Infrastructure Centric	None
Packet Encapsulation	Internal	Infrastructure Centric	None
Out-of-band Channel	External	Node Centric	Out-of-band link
High Power Transmission	External	Node Centric	High energy source
Packet Relay	Internal	Node Centric	None
Protocol Deviations	Internal	No Back-off's	None

The basic functionalities of this module are the attacker positioning, attacker compromising, attacker attacking and attacker threatening. The attacker establishes in the sensor environment with the following basic functionalities as in figure 2 and the attacker establishes in the sensor environment with the following input output interfaces as in figure 3.

Figure 2 basic Functionalities of establishment Module

Figure 3 Input Output interface of Attack Establishment Module

The wormhole attack can be eliminated by step-by-step prevention system: neighbor node list generation provided by the membership service and wormhole detection, wormhole isolation, wormhole prevention provided by the communication service. The membership service is the component in charge of keeping an updated list of the group members, processing joins and leaves of the group, and assessing the failure of members. The communication service provides primitives for data transmission in the group, like reliable data transfer, causal order or total order broadcast and data forwarding, monitoring the network group, alerting the network group of the malicious encounter if the threshold limit exceeds. This module detects isolates and further eliminates further attacks by the attacker.

The membership service of the guard nodes builds the neighbor list by a one-hop broadcast of the "HELLO" message. The node accepts the reply within the timestamp T_{RT}. A dynamic neighbor table (N_T) is maintained and updated with the information of the one-hop and the two-hop neighbor list, dynamically based on the node distributions. The shared key authenticates this broadcast individually with each member in N_T. The entire neighbor list table is built within the time period of T_{ND}.

a. Sub-Component1: 2-HopGenerator:

For a node, say G, to be able to watch and guard a node, say N1, two conditions must be satisfied: (i) each packet forwarder must explicitly announce the immediate source of the packet it is forwarding, i.e., the node from which it receives the packet, and (ii) G must be a neighbor of both N1 and the previous hop from N1, say N2. If the second condition is satisfied, we call G the guard node for the link from N1 to N2. This implies that G is the guard node for all N1's outgoing links.

b. Sub-Component2: Detecting Attacker:

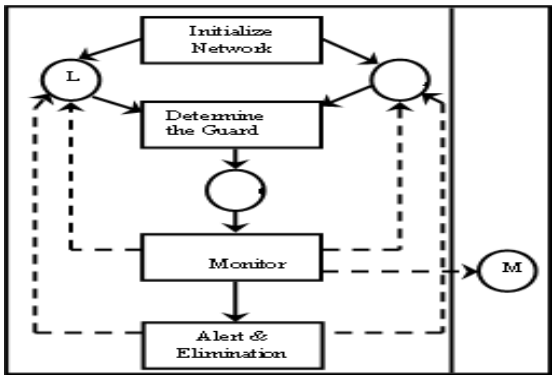

Figure: 4

Upon Collaborative Local Monitoring, any malicious node M compromising as a Neighbor is detecting during Control Packet Forwarding Process or Authentication to the Control Packets Process or Data Packet Forwarding Process or the Authentication Process by the verification with the Neighbor List Routing Table in the watch buffer information packet. The information includes packet identification, packet type, packet source, packet destination, packet immediate receiver and timestamp (t).

c. Sub-Component3: Isolating Attacker:

Upon monitoring if the malicious node M sends 1 malicious message for every 5 legitimate messages, then the node is enlisted a high priority to be monitored. The malicious counter is initiated and incremented for every malicious attack by the node M. When it exceeds the threshold limit of 1 error for every 5 correct messages, that is 20% malicious activity shown by the attacker, then the node is delineated from the Neighbor List Table. The guard node maintains malicious counter ($Mal_C(G,N)$), for each sensor node N, a guard node G monitors the sensor node N. The malicious counter is incremented depending on the nature of the malicious activity sensed. The malicious activity is detected with two parameters V_f for fabricating and V_d for dropping a control packet. When this malicious counter exceeds the threshold limit T_L, the alert buffer is activated.

d. Sub-Component4: Preventing Attacker:

After compromising and entering into the network the malicious nodes will drop data packets, delay the data packet transfer, eavesdrop the messages, causes disruptions to routing, and contributes to faulty data. When the node N gets enough alert messages, exceeding the detection confidence index of D, the minimum number of guard nodes that must report that a certain node is malicious for a neighbor of that node to isolate it, then the adversary node is eliminated.

IV. ROUTING ALGORITHMS

The wormhole attack can be eliminated by step-by-step prevention system: neighbor node list generation provided by the membership service and wormhole detection, wormhole isolation, wormhole prevention provided by the communication service. The membership service is the component in charge of keeping an updated list of the group members, processing joins and leaves of the group, and assessing the failure of members. The communication service provides primitives for data transmission in the group, like reliable data transfer, causal order or total order broadcast and data forwarding, monitoring the network group, alerting the network group of the malicious encounter if the threshold limit exceeds

A. Neighbor Node List Generation:

Initialize the sensor network topology deploying the legitimate nodes in the field. Generate 1-hop neighbor list of the legitimate nodes in the field.
Step 1: Node A (say) is deployed in the field.
Step 2: Node A does a one-hop broadcast of a HELLO message broadcast to all its 1-hop neighbors in the field.
Step 3: Any node, say B hears the message.
Step 4: Node B sends back an authenticated reply to node A, using the shared key.
Step 5: If node B responds within a timeout
Then Node A accepts the authentication message from node B Else Node A ignores the authentication message from node B.
Step 6: For each reply, node A verifies the authenticity of the reply.
Step 7: If valid authenticity, the node A adds the responder to its neighbor list NL_{1A}.
Step 8: If invalid authenticity, the node A ignores the responder.
Thus at the end of this neighbor discovery process, each node has a list of its direct neighbors built as the neighbor list table NL_{1A}. After the 1-hop neighbor list generation, generate 2-hop neighbor list of the legitimate nodes in the field.
Step 1: Node A does a 1-hop broadcast of a message containing NL_{1A} to all its 1-hop neighbors.
Step 2:Each member in NL_{1A} will individually authenticate this broadcast by the shared key.
Step 3: When node B hears the broadcast, node B verifies the authenticity of NL_{1A}.
Step 4: If verification correct
Then Node B checks, <If any duplicates> Then Node B deletes the duplicates and stores NL_{1A} received as the 2-hop neighbors in the 2-hop neighbor list of Node B as NL_{2B}.
Else Node B stores the NL_{1A} as such as the 2-hop neighbors in the 2-hop neighbor list of Node B as NL_{2B}.

B. Guard Node List Generation:

For the deployed sensor network, determine the guard nodes for every pair of the legitimate nodes. Thus at the end of this guard node discovery process, each node has a list of its guard nodes built as the guard node list table NL_{GA}.
Step 1: Node A is deployed in the field with its NL_{1A} and NL_{2A}.
Step 2: Node A does a one-hop broadcast of a GUARD message broadcast to all nodes in NL_{1A}.
Step 3: Any node, say B in the NL_{1A} hears the message.
Step 4: Node B sends back an authenticated reply to node A, using the shared key.
Step 5: If node B responds within a timeout Then Node A accepts the authentication message from node B
Else Node A ignores the authentication message from node B.
Step 6: For each reply, node A verifies the authenticity of the reply.
Step 7: If valid authenticity, node A adds the responder to its guard node table list NL_{GA}.
Step 8: If invalid authenticity, the node A ignores the responder.

V. IMPLEMENTATION

The software developed is to detect the attack in the wireless sensor networks. The basic modules to be implemented are Topology Establishment Module, Attack Establishment Module, and Elimination Management Module.

Hybrid routing algorithm is used that provides the common solution and it makes use of On-demand ad hoc routing protocol (AODV).

A. Hop Count Based Detection (Alternate Route):

In many localization schemes, average hop size is used to estimate the hop distance between nodes. There are 2 terms that should be analyzed for the worm hole attack detection. In general, average hop size is computed as:

$$hopsize_i = \frac{\sum_{j \neq i} \sqrt{(x_i - x_j)^2 + (y_i - y_j)^2}}{\sum_{j \neq i} h_j}, \quad i \neq j$$

Where (x_i , y_i), (x_j , y_j) are the coordinates of nodes i and j , and h_j is the hop count between them.

Wormhole attack generally affects the routing at network layer. It also degrades the security services at the physical layer. This technique is used to detect and isolate the wormhole attack at physical layer.

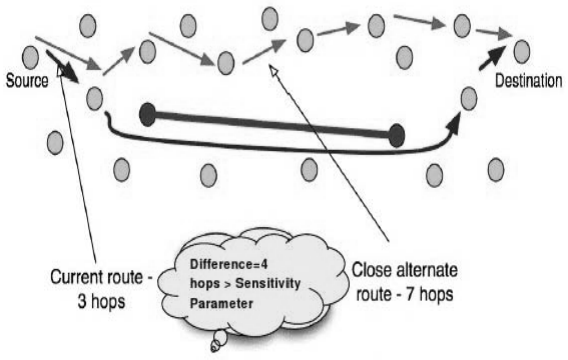

Figure 4 Detection of Wormhole

The sender node S in Figure 4 will initially have a route to the destination node D and wishes to test whether this route includes a wormhole or not. Detecting such wormholes is extremely difficult progress. The sender S will start by discovering his one-hop neighbors. Based on the received replies, sender will create a list of his one-hop neighbors that excludes the next hop along the route. The sender will check the routes (referred as test routes) that are used by these one-hop neighbors to the second hop along the route to the destination (throughout this technique we will refer to this node as the target node). Node S compares the length of a selected route with the one he has to the target node.

The selected route is chosen from the routes reported from the neighbors. If the difference between the numbers of hops of the two routes is greater than a certain value called the "Threshold value", the sender will assume that a wormhole exists. If not, this process is repeated by each node that lies on the route (such nodes also exclude the previous hop from the list). The idea is that when a node that is close to M1 is reached, its next hop neighbor along the route will be on the other side of the wormhole link (near M2)[the link in dark red color connected between two nodes called as M1 and M2]. If at least one of the \perceived" one-hop neighbors is located within the transmission range of the node, (i.e., it is not on the other side of the wormhole), the route from this neighbor to the target node can be rendered very different (typically long) and thus the wormhole will be detected.

B. Neighbor List Based Detection:

In this method secure neighbor discovery from source to destination obtained by neighbor list and detect the anomaly if attack is present. The steps are

a. One-hop neighbor discovery;
b. Initial route discovery
c. Data dissemination and wormhole detection, and
d. Secure route discovery against a wormhole attack.

Each node sends a hello message for the neighbor discovery immediately after the deployment of the mobile nodes. Each node that receives a hello message sends a reply. Each node builds its neighbor list which could include remote neighbors connected by a wormhole. The neighboring nodes exchange their neighbor lists. Each node will compare its neighbor list with its neighbors' neighbor list. If they are similar, either these nodes are close enough or are connected by a wormhole. Next, both of these nodes and their neighbors will reconstruct their neighbor lists which will remove these two nodes and their neighbors. Finally, to secure the data dissemination between neighbors, we build a pair-wise shared key using the initial key KI and random function f.

C. Detection Procedure:

Broadcast its own probe message
for each probe message received and not (TIMEOUT or WORMHOLE DETECTED) **do**
extract id, hopcount and (xj , yj) from probe message
if id $\in$ Q then
drop (probe message)
else
Q = Q+{id}
hopcount = hopcount +1
if SQRT $((x_i-x_j)^2+(y_i-y_j)^2)$ - hopcount X R > 0 **then**
send alarm message to base station.
else
Forward (probe message) to MAC
end if
end if
end for

VI. RESULTS AND DISCUSSION

In this work, the various modules have been implemented using Network Simulator Version 2 (ns2) in the network layer, where the mobile nodes have been established in the WSN topology. The analysis of the trace files generated by the backoff and the high power transmitter attack by the malicious nodes in the network simulator shows that the throughput before attack in the routing layer is 0.99 and after the attack throughput is reduced to 0.96.

The Guard nodes have been determined for this wireless sensor network topology with the ratio of 4:1. For every 4 nodes in the scenario, there exists 1 Guard node monitoring the nodes in the wireless sensor network scenario. The guard nodes are determined by using the Round Trip Time obtained from the neighboring nodes and are manipulated to provide the nearest neighbor as the next Guard Node.

Simulation can be performed in terms of Avg End-to-End delay, routing over head, Packet delivery ratio.

A. Simulation Parameters:

Table 2: Simulation Parameters

Parameter	Value
Simulator	NS-2 (ver: 2.34)
Time	300s
Total number of nodes	150
Routing Protocol	AODV
Traffic Model	CBR
Terrain Area	600m x 600m
Transmission Range	250m

B. Simulation Screenshots:

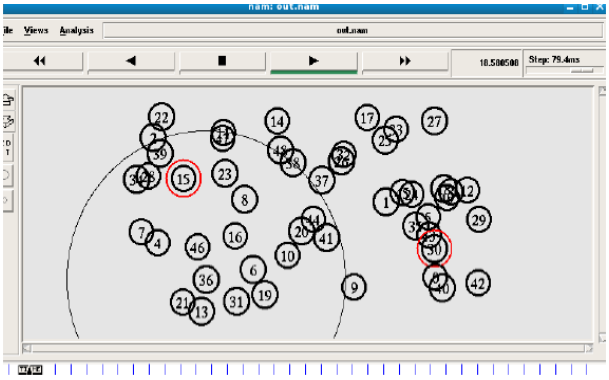

Figure:5

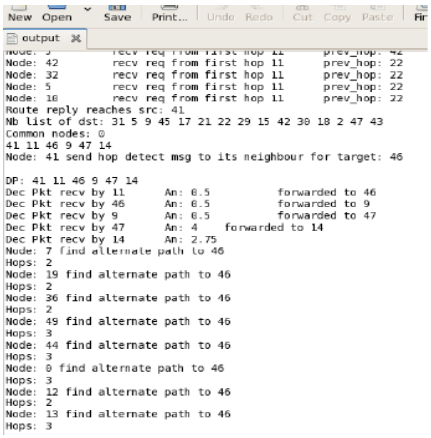

Figure: 6

VII. CONCLUSION AND FUTURE WORK

Attackers exploits wormholes to selectively drop packets, to build bogus route information, to create routing loops to waste the energy of network, to gain unauthorized access, to disrupt routing, to perform denial of service attacks, to blackmail a good node and induce rushing attack.

In this project, the attackers selectively drop packet, replays the data packets, gain unauthorized access and transmit data packets at high energy. The implemented solution of "Secure Routing Algorithms for Detecting Wormhole Attacks in Wireless Sensor Networks" solves the problem of this resource consumption wormhole attack that is induced by creating wormholes in the wireless sensor networks.

The extension of this protocol is to detect, isolate and prevent other route disruption attacks like Byzantine, Sinkhole (Blackhole) and Sybil are under work. Preventing these attacks solves the problem of routing the legitimate packets in the dysfunctional way.

VIII. REFERENCES

[1] Junfeng Wu, Honglong Chen, Wei Lou and Zhibo Wang, "Label-Based DV-Hop Localization AgainstWormhole Attacks in Wireless Sensor Networks" in IEEE Transactions, 978-0-7695-4134-1/10,2010

[2] He Ronghui, Ma Guoqing, Wang Chunlei, and Fang Lan "Detecting and Locating Wormhole Attacks in Wireless Sensor Networks Using Beacon Nodes" in World Academy of Science, Engineering and Technology 55 2009

[3] Y.C. Hu, A. Perrig, and D.B. Johnson. Packet leashes, "A defense against wormhole attacks in wireless ad hoc networks," in Proceedings of INFOCOM 2003, April 2003

[4] Issa Khalil, Saurabh Bagchi,Ness B.Shroff, "LITEWORP: A Lightweight Countermeasyre for the Wormhole Attack in Multihop Wireless Networks" on International Conference on Dependable Systems and Networks (DSN'05)

[5] Zaw Tun and Aung Htein Maw,"Wormhole Attack Detection in Wireless Sensor Networks" in World Academy of Science, Engineering and Technology 46 2008

[6] B. Dahill, B. N. Levine, E. Royer, and C. Shields, "A secure routing protocol for ad-hoc networks," Electrical Engineering and Computer Science, University of Michigan,Tech. Rep. UM-CS-2001-037, August 2001.

[7] P. Papadimitratos and Z. Haas, "Secure routing for mobile ad hoc networks," in SCS Communication Networks and Distributed Systems Modeling and Simulation Conference (CNDS), 2002.

[8] Y. C. Hu, A. Perrig, and D.B. Johnson, "Packet leashes: a defense against wormhole attacks in wireless networks," in Proceedings of the 22nd INFOCOM, pp. 1976-1986, 2003.

[9] C. E. Perkins and P. Bhagwat, "Highly dynamic destinationsequenced distance-vector routing (DSDV) for mobile computers," In ACM SIGCOMM on Communications Architectures, Protocols and Applications, 1994.

[10] D. Johnson, D. Maltz, and J. Broch, "The Dynamic Source Routing Protocol for Multihop Wireless Ad Hoc Networks," in Ad Hoc Networking, Addison-Wesley, 2001.

[11] C. Karlof and D. Wagner, "Secure Routing in Sensor Networks: Attacks and Countermeasures," at the 1st IEEE International Workshop on Sensor Network Protocols and Applications, 2003.

[12] S. Marti, T. J. Giuli, K. Lai, and M. Baker, "Mitigating routing misbehavior in mobile ad hoc networks," at the 6th ACM MobiCOM, 2000.

[13] Dhara Buch and Devesh, "Prevention of wormhole attack in wireless sensor network" on International Journal of Network Security and its Applications (IJBSA) , vol.3, Sep 2011

[14] I.F. Akylidiz, W.Su, Y. Sankarubramaniam, E. Cayiric, "A Survey on Sensor Networks" in IEEE Computer Magazine, August 2002. pp.102-114.

[15] L. Buttyán, L. Dóra, I. Vajda, "Statistical Wormhole Detection in Sensor Networks" in Second European Workshop on Security and Privacy in Ad Hoc and Sensor Networks (ESAS 2005), Visegrád, Hungary, July 13-14, 2005,pp. 128-141