STUDY OF SMART PHONE CLOUD DATA ATTACKS DETECTION AND PREVENTION

A. Sankaran*

B. Gobinathan**

Abstract: *In this paper, a platform "detecting and preventing cloud data attacks in smart phone" is proposed to support mobile smart phones accessing into wireless sensor networks (WSNs). The resource constrained ad hoc wireless sensor network is versatile yet vulnerable to attacks. Since phones have different platforms, e.g. operating systems and CPU processors, it is a challenge to provide a universal platform for smart phones. A particularly devastating attack, predominant in today's world is the wormhole attack. 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.*

*Assistant Professor, Department of Information Technology, Anand Institute of Engineering and Technology, Chennai

**Assistant Professor, Department Of Instrumentation And Communication Engineering, Indira Institute of Engineering And Technology

I. INTRODUCTION

In wireless sensor networks (WSNs), sink mobility can effectively improve data load balance and energy consumption uniformity. Currently, mobile smart phones are equipped with more powerful processors, which are able to provide novel services. With the sufficient computation capability, smart phones can play the role of mobile data sink in WSNs. Compared with manufacturing a special WSNs data sink, the phone-based data sink can save the cost largely. 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 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. SYSTEMARCHITECTURE

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. 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.

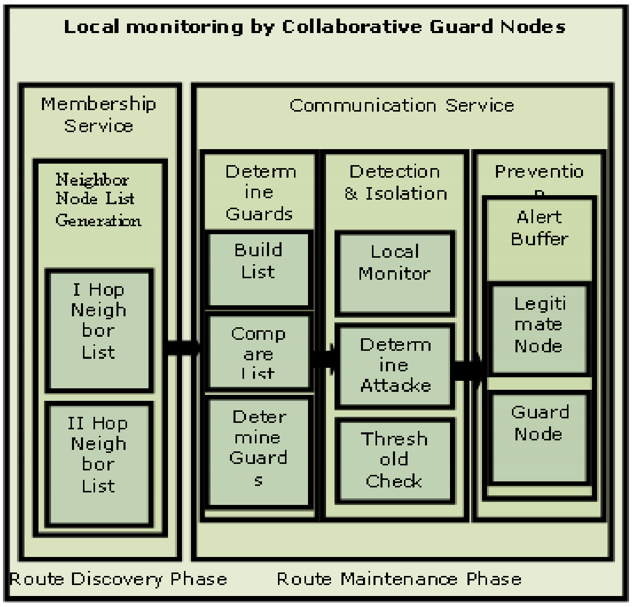

Fig. 1.Figure 1 Modular Decomposition of the software

B. Implementation Techniques:

a. 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

b. 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

c. Sub-Component 3: Control Packet Routing: must be large, and so the edge effects due to $2\Pi r$ will be negligible.

The first hop neighbor node must authenticate to the received control packet from the sender node within a time bound 5ms. 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.

d. 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-offs	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 fig 3.

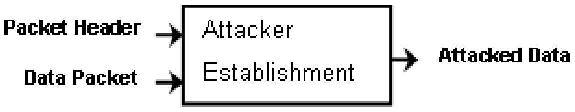

Figure 2& 3 basic Functionalities of establishment & Input Output interface of Attack Establishment Module

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.

b. Sub-Component2: Detecting Attacker:

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).

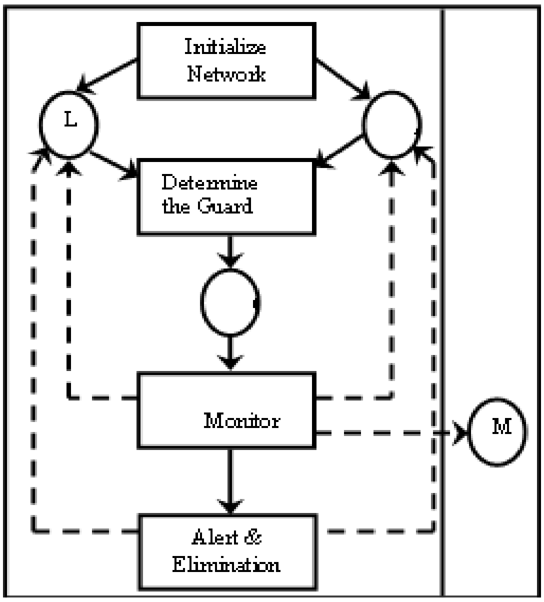

Fig. 4.Detecting Attacker

`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.

III. 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.

IV. 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.

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.

The sender node S in Figure 5 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.

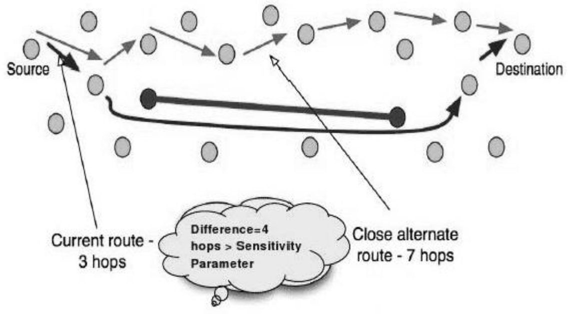
Source
Destination
Current route - 3 hops
Difference=4 hops > Sensitivity Parameter
Close alternate route - 7 hops

Figure 5 Detection of Wormhole

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,

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 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
```

V. CONCLUSION AND FUTUREWORK

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 in smart phones” 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. Preventing these attacks solves the problem of routing the legitimate packets in the dysfunctional way.

REFERENCES

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

[2] HeRonghui, 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] Issa Khalil, SaurabhBagchi, NessB.Shroff, “LITEWORP: A Lightweight Counter measure for the Wormhole Attack in Multi-hop Wireless Networks” on International Conference on Dependable Systems and Networks (DSN’05)

[4] T. Pering, P. Zhang, R. Chaudhri, Y. Anokwa, and R. Want, “The PSI Board: Realizing a Phone-Centric Body Sensor Network,” *Proc. 4th BSN2007*, Germany.

[5] A. Teot, G. Singhl, and J. C. McEachent, “Evaluation of the XMeshrouting protocol in wireless sensor networks,” *49th IEEE International Midwest Symposium on Circuits and Systems(MWSCAS ’06)*, San Juan, August 2006.

[6]The Observer pattern, “http://en.wikipedia.org/ wiki/Observer pattern”.

AUTHORS PROFILE

A.Sankaran is currently working as Assistant Professor in Anand Institute of Engineering And Technology, Chennai. Did his **M.E.** in Computer Science Engineering from Indira Institute Of Engineering And Technology, Thiruvallur, **B.E.** degree in Computer Science engineering from Adhiparasakthi Engineering College, Diploma in Electronics and Communication Engineering from Adhiparasakthi Polytechnic College. His research interest includes Artificial Intelligence, Neural Networks, fuzzy logic, Wireless communication (**WiFi, WiMax**), Mobile Computing, Sensor Networks, and Communication networks etc. And published various technical paper in National/International conferences, International journals.

B.Gobinathan, is currently working Assistant Professor, Department Of Instrumentation And Communication Engineering, Indira Institute Of Engineering And Technology, and has over 11 years of teaching and research experience. He is doing his Ph.D degree in Image Processing. His areas of interests are Image Processing, Cloud computing. He has attended many workshops and seminars. He has completed his post graduate(M.E-2011, M Phil-2007, MCA-2002) in CSE .