ISSN 2278 - 8875
International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering
Vol. 1, Issue 2, August 2012

Spying In Wireless Sensor Network to Catch Misbehaviour Nodes

G.Gurusamy[1], S.Shaik Majeeth[2], G.Ashok kumar[3]

PG Student, Saveetha Engineering College, Chennai, India[1]

Associate Professor, Department of ECE, Saveetha Engineering College, Chennai, India [2]

Assistant Professor, Department of CSE, Karpagam College of Engineering, Coimbatore, India [3]

ABSTRACT: Packet droppers and Modifiers are the intruder nodes in a multihop wireless sensor network. These attacker nodes are the intermediate nodes which drop or modifies certain data packets in the middle there by reduces the reporting probability of a sensor network. To address this problem, it proposes a scheme which can identify effectiveness and efficiency of the scheme.

KEYWORDS: Packet dropping, packet modification, intruder detection, wireless sensor networks**.**

I.INTRODUCTION

A Group of sensor nodes deployed in environment to establish wireless sensor network which is used to measure the data. Node has five components such as controller, memory, sensor and actuators, communication device, and power supply. Controller process the relevant data, capable of executing code. Memory used to store program and data. Sensor and actuator can observe and control physical parameters of the environment. Communication device used for send and receive the data. Power supply provides energy to environment.

A sensor network is deployed in environment to perform the monitoring and data collection tasks. Sensor nodes detect events, produce data, and forwarding the data toward a sink. When it forwards its data towards sink, it lacks in physical protection and node might be compromise. Among these attacks, two common ones are dropping packets and modifying packets. A compromised node drops all or some of the packets that it is supposed to forward. It may also drop the data generated by itself for some malicious purpose such as accusing innocent nodes. A compromised node modifies all or some of the packets that it is supposed to forward.

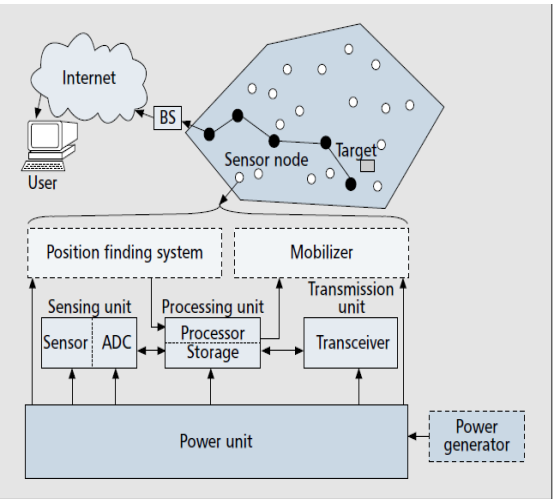

Figure 1.1 components of nodes

To deal with packet droppers, it uses counter- measure multipath forwarding [1],[2],[3],[4,],[5], in which packet is forwarded along multiple redundant paths. In Existing system, to deal with packet modifiers, most of existing countermeasures [6] are used to filter modified messages within a certain number of hops. However, without identifying packet droppers and modifiers, these countermeasures cannot fully solve

ISSN 2278 - 8875
International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering
Vol. 1, Issue 2, August 2012

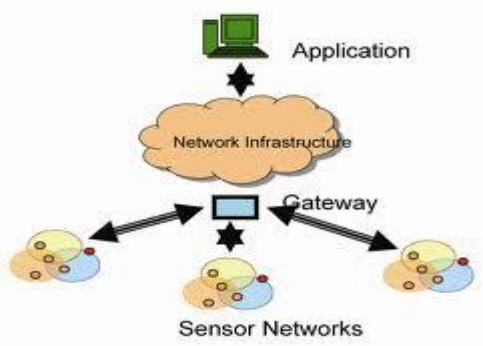

Figure 1.2wireless sensor network

the packet modification problems because the compromised nodes can continue attacking the network without being caught.

It proposed a probabilistic nested marking (PNM) scheme to identify packet modifiers with a certain probability. However, PNM [7] scheme cannot be used together with existing false packet filtering schemes because it identifies the packet modifiers or droppers in network only. It doesn't identify the intruder in the network.

It proposes node categorization algorithm to identify the packet dropper or modifiers i.e. intruder in network. According to the scheme, Sink generate pair wise key between sink and every sensor node, and a dynamic routing tree rooted at the sink is established. When sensor data is transmitted along the tree structure towards the sink, each node which may be sender or forwarder adds a small number of extra bits to the packet .It called as packets marks. The format of the small packet marks is designed in such way that the sink can obtain very useful information from the marks.
Based on the packet marks, the sink can figure out the dropping rate associated with every sensor node, and then run proposed node categorization algorithm to identify nodes that are droppers/ modifiers for sure or are suspicious droppers/modifiers. Tree structure dynamically changes for every round, behaviours of sensor nodes can be observed in a large variety of scenarios. It also use heuristic ranking algorithm to identify bad nodes from suspicious node.

II. PROBLEM STATEMENT

A WSN is composed of sensors. When it is deployed in environment to perform monitoring, detect event, sense data and forward those data towards sink. At the time of forwarding data to its parent node might be misbehaviour node [8]. (i.e.) modify or drop the data.

Two types of misbehaviour node one is selfish behaviour node and another is malicious behaviour node. Selfish behaviour node e.g. node want to save power, CPU cycles and memory. Malicious behaviour node attack and damage the network. In packet forwarding malicious behaviour node further classified into two types forwarding and routing. Forwarding misbehaviour are packet modification, dropping, timing attacks and route change. Timing attack is an attack in which malicious node delays packet forwarding to ensure that packet expires their time to live (TTL).
Routing misbehaviour attacks during the route discovery phase. Three common attacks such as black hole, gray hole, and worm hole. In black hole attack, malicious node claims to have shortest path and drop the packet in route. In a gray hole attack, malicious node selectively drop the packets. In a wormhole attack, malicious node send packet from one part to another part of network where reputation of packets.

ISSN 2278 - 8875
International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering
Vol. 1, Issue 2, August 2012

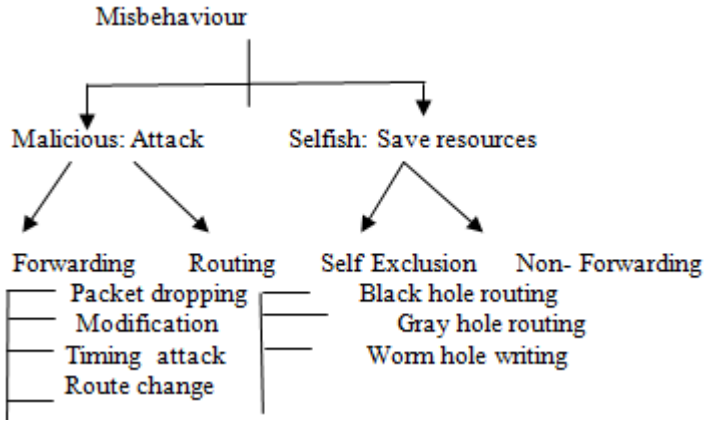

Figure 1.3 Misbehavior classification

Selfish behaviour node classified as self- exclusion and non-forwarding node. In self-exclusion misbehavior, a selfish node doesnot participate during route discovery.
Non –forwarding misbehaviour is one in which a selfish node fullyparticipated in route discovery phase but refuses to forward the packets.
It [2] focuses on routing security in wireless sensor networks. Existing proposals for routing protocols in sensor networks optimize for the limited capabilities of the nodes and the application specific nature of the networks, but do not consider security. It [3] classified WSN traffic into one of three categories
Many-to-one: Many sensor nodes send readings to a base station or aggregation point in the network.
One-to-many: A single node (typically a base station or an aggregator) floods several sensor nodes with query or control information.
Local communication: Neighbouring nodes send localized messages to discover and coordinate tasks.

III .SYSTEM MODEL

a. Network Assumption
It considers a typical deployment of sensor network, as shown in Fig. 3.1, where a large number of sensor nodes are deployed in area. Network structure is established from directed acyclic graph (DAG).A Directed Acyclic Graph (DAG) is a directed graph with no directed cycles. It is formed by a collection of vertices and directed edges, each edge connecting one vertex to another, such that there is no way to start at some vertex *v* and follow a sequence of edges that eventually loops back to *v* again.

Each sensor node generates data from environment periodically and all these nodes forward packets that contain the data hop by hop towards a sink. The sink is located as root node within the network. It assumes that all sensor nodes and the sink are time synchronized. The sink is aware of the network topology extracted from DAG.

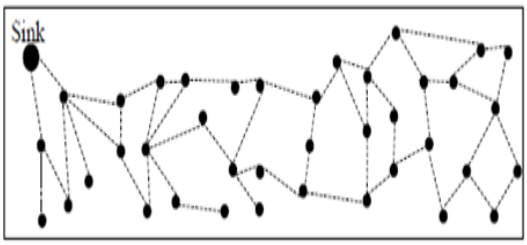

Figure 3.1 system Assumption

b.security Assumption and Attack Model
It assumes the network sink is trustworthy and free of compromise, but regular sensor nodes can be compromised. Compromised nodes may or may not collude with each other. A compromised node can launch the following two attacks:
Packet Dropping
A misbehaviour node drops all or some of the packets that it is supposed to forward. It may also drop the data

ISSN 2278 - 8875
International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering
Vol. 1, Issue 2, August 2012

generated by itself for some malicious purpose.

Packet Modification

A misbehaviour node modifies all or some of the packets that it is supposed to forward. It may also modify the data generates by itself.

IV. ARCHITECTURE

a. Proposed Model

It proposes a simple yet effective scheme to catch both packet droppers and modifiers. According to the scheme, Sink generate pair wise key between sink and every sensor node, and routing tree rooted at the sink is established. When sensor data is transmitted along the tree structure towards the sink, each intermediate node adds a packet marks to the original packet.

Based on the packet marks, the sink can figure out the dropping rate associated with every sensor node, and then run our proposed node categorization algorithm to identify nodes that are droppers/ modifiers for sure or are suspicious droppers/modifiers

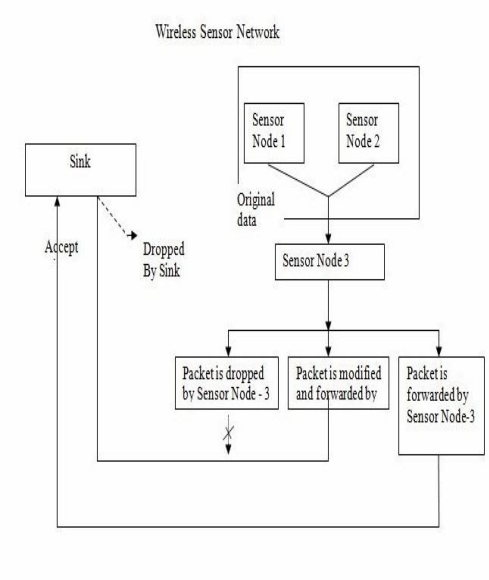

Figure 4.1 proposed Architecture

Consider fig 4.1 sensor node 1 and 2 sense data periodically and forward those data hop by hop towards sink. Sensor node 3 receives data from its parent and forwards it to sink .If intermediate node modifies the original data from the source to destination then the corresponding data packet is discarded by sink or else the data packet is delivered successfully.

b. Key Generation

To setup secret pair wise key between the sink and every sensor node. Establish the tree to forward packets from every sensor node to the sink. Tree is established from directed acyclic graph.

Key is symmetric which is used for both encryption and decryption of data. It is shared between sink and every sensor node.

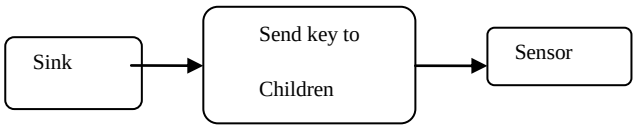

Figure 4.2 Key Generation

c.Node Categorization Algorithm

In the initialization phase, sensor nodes form a dynamic routing tree rooted at the sink. The structure of the tree changes dynamically from round to round. In each round, data traffic is transmitted through the routing tree to the sink, and each packet sender/forwarder adds a small number of extra bits to the packet and also encrypts the packet.

When one round finishes, based on the extra bits carried in the received packets, the sink runs the node categorization algorithm [9] to identify nodes that must be droppers or modifiers and nodes that are suspiciously bad. The routing tree which is extracted from DAG reshaped every round.

Dropping ratio is calculated as follows:

$d_{u=} n_{u,\ flip*Ns} + n_{u,\ max} + 1 - n_{u,\ rec}$

ISSN 2278 - 8875
International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering
Vol. 1, Issue 2, August 2012

$n_{u, flip*Ns} + n_{u, max}$
The first step of the identification is to mark each node with "+" if it's dropping ratio is lower than Θ, or with "-"otherwise.
Case 1 :+{+}
The parent and its child marked as "+". If two nodes marked as "+" in sequence then it does not drop packets along the involved path but it doesn't know whether they drop the packets on other forwarding paths. Sink identifies these types of nodes are *temporarily good.*

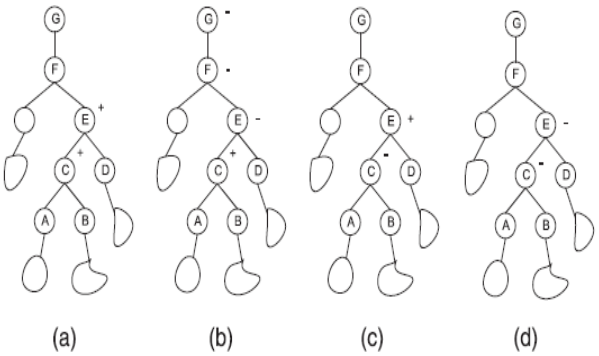

Figure 4.3 Node Categorization Algorithm

Case 2 :+-{-}
The parent node marked as "+" and following its child marked as "-".Sink identifies these types of nodes are *bad for sure.*
Case 3 :-{+}
In this case either the node marked as"-"or its parent marked as"+" must be bad but sink does not identify whether node with "-"is bad or node with "+"is bad and both nodes are bad. So sink identifies these types of nodes are *suspiciously bad.*
Case 4 :-{-}
The parent and its child marked as "-".If two nodes marked as "-" in sequence. Sink identifies these types of nodes are *suspiciously bad.*

c. Packet Format and Identifying Modifier
Each node maintains a counter C_p which keeps track of the number of packets that it has sent so far. When a sensor node u has a data item D to report, it composes and sends the following packet to its parent node P_u. Packet format is $<P_u, \{R_u, u, C_P \text{ MOD } N_s, D, pad_{u,0}\} K_u, pad_{u,1}>$
Consider 0 as a Sink and Sensor node-6 is sender, see in the below Diagram, When the sink receives a packet, it conducts the following steps:
The sink attempts to find out a child of it, such that results in a string starting with Rv (Random number), means the result of decrypting m with key *Kv*.
If attempt fails, the packet is identified as being modified and thus should be dropped. If attempt succeeds, it indicates that the packet was forwarded from that node.
There are two cases if finally decrypted Packet starts with R (Random) it indicates that node *v* is the original sender of the packet. Otherwise, it indicates that node *v* is an intermediate forwarder of the packet.

ISSN 2278 - 8875
International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering
Vol. 1, Issue 2, August 2012

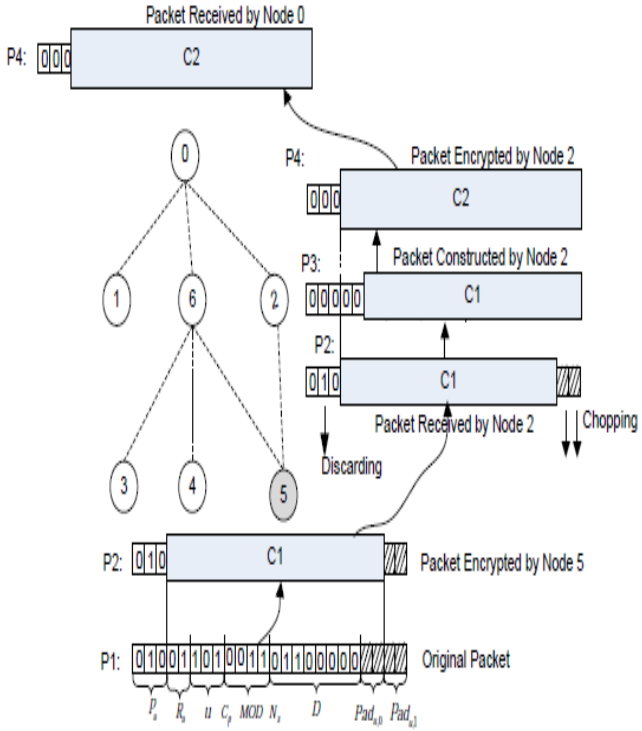

Figure 4.4 Packet Format and Forwarding

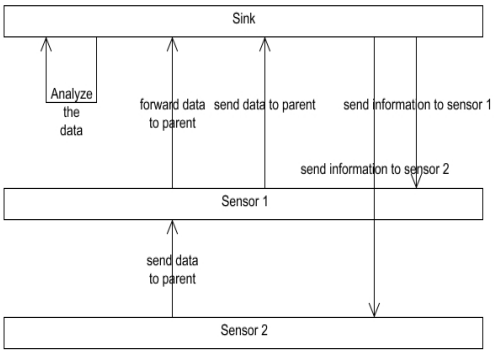

Figure 4.5 Identifying Modifier

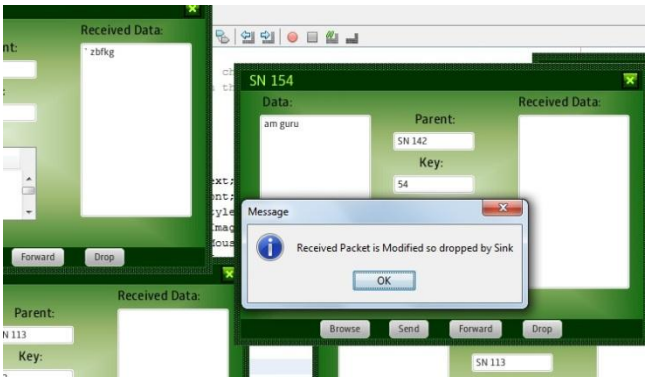

Figure 4.5 simulation Result

Consider fig 4.5 sensor nodes sense data periodically and forward those data hop by hop towards sink. A sensor node receives data from its parent and forwards it to sink. Intermediate node modifies the original data from the source to destination so the corresponding data packet is discarded by sink.

D .Identify Packet Dropper

The Node Categorization Algorithm is used in this System. In every round, for each sensor node *u*, the sink keeps track of the number of packets sent from *u*, the sequence numbers of these packets and the number of flips in the sequence numbers of these packets. In the end of each round, the sink calculates the dropping rate for each node.
Based on the dropping rate of every sensor node and the tree topology, the sink identifies the nodes that are droppers for sure.

V. CONCLUSION

To address the problem of packet dropping and modification, it proposed a simple effective scheme to identify misbehaving forwarders that drop and modify packets. Each packet is encrypted and padded so it hides the source of data. Packet mark added in each packet so sink can recover the source of the packet and figure out the dropping ratio associated with each and every sensor node. The routing tree changes dynamically for each round. Finally, most bad nodes identified by node categorization algorithm with small false positive. Extensive analysis, simulation, and implementation have been conducted and verified the effectiveness of proposed scheme.

REFERENCES

[1] H.Chan and A. Perrig, "Security and Privacy in Sensor Networks," IEEE Computer, October 2003.
[2] C. Karlof and D. Wagner, "Secure routing in wireless sensor networks: attacks and countermeasures," the First IEEE International Workshopon Sensor Network Protocols and Applications, pp. 113–127, May 2003.
[3] V. Bhuse, A. Gupta, and L. Lilien, "DPDSD: Detection of packet-dropping attacks for wireless sensor networks," In the Trusted Internet Workshop, International Conference on High Performance Computing, December 2005.
[4] S. Marti, T. Giuli, K. Lai, and M. Baker, "Mitigating Routing Misbehaviour in Mobile Ad Hoc Networks," ACM MobiCom, August 2000.
[5] S. Lee and Y. Choi, "A resilient packet-forwarding scheme against maliciously packet-dropping nodes in sensor networks," Proceedings of the fourth ACM workshop on Security of ad hoc and sensor networks (SASN), pp. 59–70, and 2006.
[6] F. Ye, H. Luo, S. Lu, and L. Zhang, "Statistical En-route Filtering of Injected False Data in Sensor Networks," IEEE INFOCOM, March 2004.
[7] F.Ye, H.Yang, and Z.Liu, "catching moles in sensor networks"proc.27th Int'l conf. Distributed computing system (ICDCS '07), 2007.
[8]A.Srinivasan, J.Teitelbaum, "Reputation and Trust based system for adhoc and sensor network" 2007.
[9] C.Wang, T.Feng, J.Kim "Catching packet droppers and modifiers in wireless sensor networks" IEEE computer society 2012.