Heuristic Method To Mitigate the Misbehaving Forwarders That Drop or Modify the Packets in WSN

Arathi C
Dept of CS&E
KVGCE, SULLIA, DK – 574327
VTU, Belgaum.

Asst. Prof. Kishore Kumar K
Dept of CS&E
KVGCE, SULLIA, DK – 574327
VTU, Belgaum

Dr. Antony P J
Director-PG Studies
KVGCE, SULLIA, DK – 574327
VTU, Belgaum

***Abstract* - Wireless Sensor Networks are growing very rapidly in the recent years and they are the most targeted subject for attacks, which can be launched by a third party to mislead the communication in wireless multi-hop sensor networks. There exist many schemes to mitigate such attacks, but very few can efficiently identify the intruders in the network. To address this problem, , this paper proposes a method that is the improved method of multipath forwarding and the method of filtering modified messages which are en-routed within certain number of hops, this method helps in identifying misbehaving forwarder nodes that drop or modify packets in WSN. In the proposed method each packet is encrypted and padded so as to hide the source of the packet, which is called as packet mark. The packet mark is a small number of extra bits that is added in each packet such that the sink can recover the source of the packet, topology of the network, by constructing a routing tree of nodes in network and then figure out the dropping ratio associated with every sensor node. The routing tree structure dynamically changes in each round so that behaviors of sensor nodes can be observed in a large variety of scenarios. Finally, most of the bad nodes can be identified by the proposed heuristic ranking and node categorization algorithms with small false positive.**

Keywords- Wireless sensor network, Multipath forwarding, Packet dropping, Packet modification and Intrusion detection.

I. INTRODUCTION

The WSN is a special class of ad hoc wireless network that are used to provide a wireless communication infrastructure that allows us to instrument, observe and respond to phenomena in the natural environment and in our physical and cyber infrastructure[1]. The WSN is built of "nodes" from a few to several hundreds or even thousands, where each node is connected to one (or sometimes several) sensors. Each such sensor network node has typically several parts: a radio transceiver with an internal antenna or connection to an external antenna, a microcontroller, an electronic circuit for interfacing with the sensors and an energy source, usually a battery or an embedded form of energy harvesting[2]. Fig. 1 represents the components of a sensor node.

WSNs are typically self-organizing and self-healing. Self-organizing networks allow a new node to automatically join the network without the need for manual intervention. Self-healing networks allow nodes to reconfigure their link associations and find alternative pathways around failed or powered-down nodes. The heart of any WSN lies in the sensors. Wireless sensor networking topologies generally fall into four categories: one-way, bi-directional, star and mesh networks. The few applications of WSNs are as environment monitoring, health monitoring, traffic control, industrial sensing, and infrastructure security.

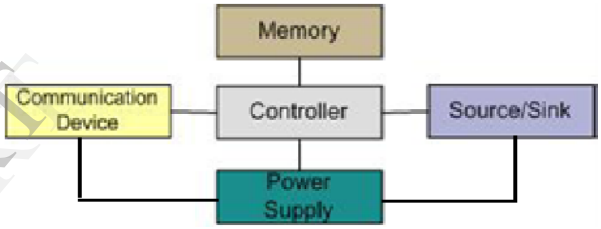

Fig. 1 Components of sensor node

The Simplicity in Wireless Sensor Network with resource constrained nodes makes them extremely vulnerable to variety of attacks. In a Wireless sensor networks sensor nodes monitor the environment, detect events of interest, produce data and collaborate in forwarding the data towards to a sink, which could be a gateway, base station or storage node. Securing the Wireless Sensor Networks need to make the network support all security properties: confidentiality, integrity, authenticity and availability. Sensor networks are often deployed in critical environment to perform monitoring and data collection. In such environment there is a lack of physical protection for the individual sensor, which results in a node compromise [3]. When a node is under compromise a third party can be able to attack a node to disrupt the communication in the established network. Hence among the attacks in a WSN most common attack are dropping and modifying the packets, which are supposed to be forwarded towards the sink. This can be stated as below

a) Packet dropping: 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.

b) Packet modification: A compromised node modifies all or some of the packets that it is supposed to forward. It may also modify the data it generates to protect itself from being identified or to accuse other nodes.

To reduce these attacks in the network, the existing methods are multipath forwarding, filtering messages en-route within certain number of hops and continuous monitoring of the neighbour nodes behaviour such as probabilistic nested marking scheme.

This paper presents a method to mitigate both packet dropper and modifiers in the established network modifiers by implementing an application to identify nodes that are droppers/modifiers for sure or are suspicious droppers/modifiers. The system can be used in all the wireless networks to have a secured network information exchange and assure the delivery of information to the destination and which can be combined with the existing multipath forwarding and filtering modified messages. The purpose of this method is to identify the system which is involved in the packet dropping and modification and route the packet in a secure path. Thus it will inform the source and destination about the packet modification and sends the suspicious node information to the network administrator and block the suspected node. The strong features of the proposed system are, it is effective scheme in identifying both packet dropper and modifiers, communication and energy overhead is low and it is compatible with the existing system.

.

II. RELATED WORK

The present approaches for detecting packet dropping and modification attacks can be categorized into three classes: multi path forwarding approach, neighbour monitoring approach, and acknowledgment approach. The following literature survey presents related work towards the problem defined.

Mitigating Routing Misbehaviour in Mobile Ad Hoc Networks, [2000] **:**S. Marti, T. Giuli, K. Lai, and M. Baker, made focus on the throughput in an ad hoc network in the presence of nodes that agree to forward packets but fail to do so[4]. To mitigate this problem, they proposed categorizing node based upon their dynamically measured behaviour. They did use of a watchdog that identifies misbehaving nodes and a path rater that helps routing protocols avoid these nodes.

Security and Privacy in Sensor Networks (vol. 36, no. 10, pp. 103-105, Oct. 2003):H. Chan and A. Perrig, addressed the problem of the security and privacy research challenges to ensure that it does not turn against those whom it is meant to benefit [5]. Hence they posed their work on the solutions of Sensor Node Compromise, Eavesdropping, Privacy Of Sensed Data, Denial-Of-Service Attacks, Malicious Use Of Commodity Networks.

DPDSN: Detection of Packet-Dropping Attacks for Wireless Sensor Networks, [2005]:V. Bhuse, A. Gupta, and L. Lilien stated the problem of Packet dropping attacks in category of DoS attacks [6]. And proposed a light weight solutions to detect such attacks on WSNs. Hence in there paper, they proposed a lightweight solution called DPDSN. which identifies paths that drop packets by using alternate paths that WSN finds earlier during route discovery. Responding to a packet-dropping attack incurs no additional cost because one of the alternate paths is utilized for all subsequent communication. DPDSN does not require monitoring individual nodes, making it feasible for WSNs. They formulate the probability of success and failure of DPDSN in the presence of malicious nodes that drop packets.

Misbehaviour Resilient Multi-Path Data Transmission in Mobile Ad-Hoc Networks,[2006]: M. Kefayati, H.R. Rabiee, S.G. Miremadi, and A. Khonsari, focused on mitigating the effects of misbehaving nodes in mobile ad-hoc networks. For that they developed scheme called APSL (Adaptive Path Selection and Loading) as a multi-path data transmission [7]. In APSL misbehaviour resilience is achieved by adaptively loading Reed-Solomon (RS) coded data into multiple node-disjoint paths. In order to maximize packet delivery ratio, paths are loaded according to Path State Information (PSI) which dynamically estimates the availability and stability of each path.

Detecting Selective Forwarding Attacks in Wireless Sensor Networks Using Two-Hops Neighbour Knowledge, [2008]: T.H. Hai and E.N. Huh, considered the problem in Selective forwarding attacks that may corrupt some mission critical applications such as military surveillance and forest fire monitoring[8]. Such as in these attacks, malicious nodes behave like normal nodes in most time but selectively drop sensitive packets, such as a packet reporting the movement of the opposing forces. Such selective dropping is hard to detect. Hence they made approach that is a lightweight security scheme for detecting selective forwarding attacks. The detection scheme uses a multi-hop acknowledgement technique to launch alarms by obtaining responses from intermediate nodes.

Coping with Node Misbehaviours in Ad Hoc Networks: A Multi-Dimensional Trust Management Approach [2010]: W. Li, A. Joshi, and T. Finin, found that the nodes in Mobile Ad hoc Networks (MANETs) are required to relay data packets to enable communication between other nodes that are not in radio range with each other. However, whether for selfish or malicious reasons, a node may fail to cooperate during the network operations or even attempt to disturb them, both of which have been recognized as misbehaviours [9]. Various trust management schemes have been studied to assess the behaviours of nodes so as to detect and mitigate node misbehaviours in MANETs.

Existing counter measures aim to filter modified messages en-route within a certain number of hops. These counter measures can tolerate or mitigate the packet dropping and modification attacks, but the intruders are still there and can continue attacking the network without being caught. In existing scheme, modified packets should not be filtered out en route because they should be used as evidence to infer packet modifiers; hence, it cannot be used together with existing packet filtering schemes.

III. PROPOSED METHOD

The proposed method in this paper includes the following procedure foe mitigating the above mention attacks in the introduction part, which goes as follows.

Based on the network established a routing tree routed at the sink is first achieved, then the sensor data is transmitted along the path towards sink, which is as mentioned by the sink itself, where each node/packet sender in the network adds a small number of extra bits which can be called as "packet mark". By which sink can figure out the dropping ratio of each node in the established network. Then the sink runs the proposed node categorization algorithm at certain interval to identify nodes that are dropper/modifier for sure/suspicious. During each round or each interval the structure of the tree dynamically changes because of this behavior of each sensor node can be observed in a large variety of scenarios. As the information of each node behavior has been accumulated at the sink, the sink periodically runs the proposed heuristic ranking algorithm to identify most likely bad nodes from suspicious nodes.

The architecture and the flow of the proposed system is as shown in below fig: 2

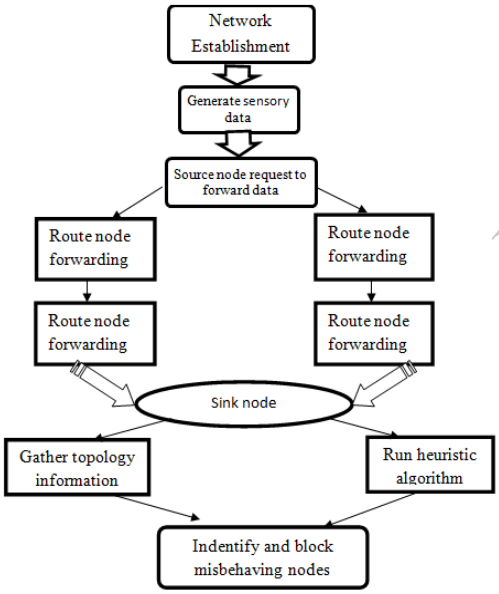

Fig.2 Architecture of the proposed method

Which start from network establishment and ends by blocking the misbehaving nodes in the path, where the data forwarding path includes many nodes called router nodes. The sensor node (source node) produces the sensory data to be forwarded to the sink node. The process includes the standard encryption and decryption algorithm.

The proposed system has the following functional modules for the identification of the node which modifies or drops the forwarded packet.

A. Network Creation Module:

The network assumption made is, the network is bidirectional, where generated sensor data by the source and all other nodes collaborate to forward data to the sink, where the sink is located within the network. All nodes are locally synchronized [11] and the sink node is aware of the established network topology. Sink is trust worthy and free from compromise, where each node is named as 'u'.

B.DAG Establishment:

The established network must be DAG, where in each round the tree is extracted from this DAG itself, data is forwarded towards the sink according to this tree. At each round the sink knows the DAG structure and the tree structure and accordingly shares a secret key with each node in the tree, after which each node in the tree uses this secret key to encrypt the packet while forwarding the data to the sink along the tree/path, and every node in the path adds a small bits called packet mark in the encryption procedure, where for the encryption procedure standard AES algorithm is used, which is a block cipher such as MARS,RC6,RIJANDUAL algorithm etc[10].On the contrary a misbehaving intermediate node may drop a packet it receives. On receiving a packet the sink decrypts the packets and finds out the original sender and packet sequence number. The sink tracks the sequence numbers of received packets for every node, and for every certain time interval, which we call a round, it calculates the packet dropping ratio for every node. Based on the dropping ratio and the knowledge of the topology, the sink identifies packet droppers based on rules we derive. Initially each sensor node 'u' is preloaded with the following parameters. Initially each sensor node 'u' is preloaded with the following parameters.

1. K_u: secret key shared between node and sink
2. L_r: Duration of each round
3. N_p: Maximum number of packets that each node can have during DAG establishment procedure
4. Ns: the maximum packet sequence number. First packet number is '0', Ns packet number is 'Ns-1', Ns+1 packet number will be '0' again.

Hence each node 'u' will be initially loaded by $u=\{K_u,L_r,N_p,N_s\}$.

Where in this phase the topology establishment is also done, after deployment sink broadcasts to its one hop neighbor a two tuple information, where in that the first field will be ID of the sender(hence initially it is sink, its ID is set to '0') and the second field will be distance hop from the sender to the sink.

C. Packet Sending and Forwarding:

In this the data are transferred through the routing tree to the sink. At each node a counter Cp is maintained, which keep count of the number if packet sent from that node. 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 a node categorization algorithm to identify nodes that must be bad (i.e., packet droppers or modifiers) and nodes that are suspiciously bad (i.e., suspected to be packet droppers and modifiers). When a sensor node u has a

data item D to report, it composes and sends the following packet to its node.

Pu: <Pu,{Ru,u,Cp MOD Ns,D,padu,0} Ku,padu,1>

Where Pu - parent node, Ru – receiving node, u- node, Cp – counter node, D – data ,pad u,0 –padding, Ku encryption. Puddings pad u,0 and pad u,1 are added to make all packets equal in length, such that forwarding nodes cannot tell packet sources based on packet length, Meanwhile, the sink can still decrypt the packet to find out the actual content.

When a sensor node v receives packet <v,m>, it composes and forwards the following packets to its parent node Pv.

Pv: <Pv,{Rv,m}Kv>

Where m is obtained by trimming the rightmost log(Np) bits off m. Meanwhile , Rv, which has logNp bits,is added to the front of m.

To make the packet more secure from the droppers the packet structure can be modified as below,

P_u:<P_u,D,MAC(D),{Ru,u,Cp,MOD,Ns,D,padu,0} Ku,padu,1>

Where MAC(D) is message authentication code for the data D from neighbors. And the forwarding packets are modified as

Pv: <Pv,D,MAC(D),{Rv,m`}Kv>

where m` is constructed in the same way from m as in the scheme to identify packet droppers.

D. Packet Receiving At The Sink

Sink receives the packet and it goes on decrypting each packet from the secret key it is shared at each node, this procedure goes downward in the tree till the leaf. If it fails to decrypt the packet for particular node's secret key it will be marked as suspicious node. To mark the node as for sure modifier the procedure will be maintained till all nodes are visited in the tree. The routing tree is reshaped every round. As a certain number of rounds have passed, the sink will have collected information about node behaviors in different routing topologies. The information includes which nodes are bad for sure, which nodes are suspiciously bad, and the nodes' topological relationship. The sink marks the bad nodes as'-' and the suspicious bad nodes as '+'. The mark pattern may have the following combination of marking of each node,

Case 1] +{+} : temporarily good node.

Case 2] +-{-} : All nodes marked as – are bad nodes for sure.

Case 3] –{+} : Either the node marked as "-" or its parent node marked as "+" is bad , hence suspiciously bad nodes. But it cannot be inferred as the node with "-" is bad or the node with "+" is bad or both are bad.

Case 4] –{-} : Every node marked with "-" could be bad or good.

To further identify bad nodes from the potentially large number of suspiciously bad nodes, the sink runs tree based node categorization algorithms .By which the sink calculate the dropping ratio of each node and it will also set threshold drop ratio as 'Θ'. The tree based node categorization algorithm is as follows

Algorithm 1. Tree-Based Node Categorization

1. Input: Tree T, each node u marked by "+" or "_" and its dropping ratio du.
2. for each leaf node u in T find parent node until the sink node categorize the nodes.
3. consider u as positive threshold and v as negative threshold.
4. If v. mark ="_"then until v.mark="+" or v is Sink, Set nodes from b to e bad for sure.
5. if v is Sink then Set u as bad for sure.
6. If v. mark ="+" and if v is not bad for sure then set u and v as suspiciously bad else
7. if dv – du>θ then
8. Set v as bad for sure.
9. if difference du-dv> θthen Set u and v as suspiciously bad;

Nu,max - most recently seen sequence number

Nu,flip - the number of sequence number flips

nu,rcv - number of received packets

E. Identifying most likely bad nodes from the suspicious bad nodes

To conclude a node as a bad for sure the probability of being bad is considered, and the sink calculates the drop ratio of each node at the end of round and for ranking each node we may consider one of the following ranking algorithms [12]: global ranking based approach, Hybrid ranking based method and stepwise ranking based method and the collision among the nodes can be considered under the horizontal collusion and vertical collusion.

V. PERFORMANCE ANALYSIS

The proposed method in this paper can be simulated in the ns-2 simulator to evaluate the effectiveness and efficiency of the proposed method. The objectives of the evaluation is carried in four subjects: Firstly testing the effectiveness and efficiency of the proposed method, secondly studying the impacts of various system parameters such as network scale, presence of bad nodes, presence of node collusion, etc. Thirdly testing the effectiveness of the proposed method for different attacks and finally comparing the throughput for each global ranking algorithm. The performance can be measured for detection rate versus false positive probability.

CONCLUSION

The proposed method in this paper is a efficient method for identifying the packet dropper and modifiers where each packet is encrypted and added by a pad to hide the source from the sink, the routing tree dynamically changes for particular interval. Finally most of the bad nodes are identified

and blocked from the path established; packets are forwarded in secure path. Extensive analysis, simulation and implementation have been made for the proposed method.

REFERENCES

[1] C. Karlof and D. Wagner. Secure Routing in Sensor Networks: Attacks and Countermeasures. In Proc. of First IEEE Workshop on Sensor Network Protocols and Applications, May 2003.

[2] On Wireless Sensor Networks: Architectures, Protocols, Applications, and Management Yazeed Al-Obaisat, Robin Braun Institute of Information and Communication Technologies University of Technology, Sydney Sydney, Australia yazeedal@eng.uts.edu.au

[3] Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures Chris Karlof David Wagner University of California at Berkeley ckarlof,daw@cs.berkeley.edu

[4] S. Marti, T. Giuli, K. Lai, and M. Baker, "Mitigating routing misbehavior in mobile ad hoc networks," in *ACM MobiCom*, 2000.

[5] H. Chan and A. Perrig, "Security and privacy in sensor networks," *Computer*, vol. 36, no. 10, 2003.

[6] V. Bhuse, A. Gupta, and L. Lilien, "Dpdsn: Detection of packet-dropping attacks for wireless sensor networks," in *the Fourth Trusted Internet Workshop*, 2005.

[7] M. Kefayati, H. R. Rabiee, S. G. Miremadi, and A. Khonsari, "Misbehavior resilient multi-path data transmission in mobile ad-hoc networks," in *ACM SASN*, 2006.

[8] T. H. Hai and E. N. Huh, "Detecting selective forwarding attacks in wireless sensor networks using two-hops neighbor knowledge," in *IEEE NCA*, 2008.

[9] W. Li, A. Joshi, and T. Finin, "Coping with node misbehaviors in ad hoc networks: A multi-dimensional trust management approach," in *IEEE Mobile Data Management*, 2010.

[10] The Advanced Encryption Standard: Rijndael K. Cartrysse and J.C.A. van der Lubbe Supplement to the books "Basic methods of cryptography" and "Basismethoden cryptografie" October 2004

[11] Q. Li and D. Rus, "Global clock synchronization in sensor networks," in *IEEE INFOCOM*, 2004.

[12] Chuang Wang, Taiming Feng, Jinsook Kim, Guiling Wang, and Wensheng Zhang, "Catching Packet Droppers and Modifiers in Wireless Sensor Networks".