A Survey and Analysis of Reliable Data Packet Delivery Ratio in Wireless Sensor Network

D.Prasanna, Research Scholar, Karpagam University, Coimbatore, TamilNadu.
Dr. G. Tholkappia Arasu, Principal, AVS Engineering College, Salem, TamilNadu.

Abstract

Wireless Sensor Networks refers to a multi-hop packet based network that contains a set of mobile sensor nodes. Every node is free to travel separately on any route and can modify its links to other nodes. Therefore, the network is self-organizing and adaptive networks which repeatedly changes its topology. The relations among nodes are restricted to their communication range, and teamwork with intermediate nodes is necessary for nodes to forward the packets to other sensor nodes beyond their communication range. Sensor networks are often deployed in unattended and hostile environments. Due to the lack of physical protection, sensor nodes are subject to node compromise. After compromising one or multiple sensor nodes, the adversary may launch various attacks to disrupt the in-network communication. It is also called packet dropping. Packet dropper and modifier are common attack that can be launched by an adversary to disrupt communication in wireless multi-hop sensor. Many techniques can be used to mitigate and tolerate such attacks but very few can effectively and efficiently identify the intruder.

Introduction

Wireless Sensor networks consist of large number of small sensor nodes having limited computation capacity, restricted memory space, limited power resource and short-rage radio communication device. Wireless sensor networks is a spatially distributed autonomous sensors based on environmental conditions like temperature, pressure and sound and other features present in wireless sensors networks, with cooperatively transfer their data throughout network communication present in the process of the each network specification process. Wireless sensors networks are achievable based on military applications present in the real time application development process in battlefield, today wireless sensor networks are used in process business and industrial applications for accessing services from process application in detecting other allowed users entered into application development. Wireless sensor network is a collection nodes with cooperative communication between systematic data transmission, in this communication every node must connect with other nodes and also connect with one sensors, each sensor network connect with realistic transmission with several ports present in the network.

Wireless sensor networks are application specific and consist of a large number of low cost, low power, resource constrained, tiny smart sensors, communicating using the wireless medium and are densely and randomly deployed with no fixed topology in remote and hostile locations. The sensor nodes are usually battery powered and possess very limited resources in terms of energy, storage, and processing capabilities. To sense, locally process the information and communicate it to the base station are the three key tasks of a sensor node. Besides providing the endless opportunities, the sensor networks also provide security challenges because of the sensitive data involved, limited battery and memory resources and unattended environment.

Sensor networks are vulnerable to a number of security attacks which can be either outside attack or inside attack [1]. Outside attacks are not very effective and not cause much damage to the network because they do not have the access to the network information. The inside attacks, on the other hand, are very effective and can disrupt the normal network functioning as the adversary is part of the network and has access to the network information. This makes it difficult to detect the adversary using traditional security mechanisms, authorization and authentication, as the adversary is legitimate member of the network. One such security attack on the sensor networks is the Selective Forwarding attack, a packet drop attack, launched with intention to suppress the important information reaching the base station. Such an attack is difficult to detect and is more effective when the attacker includes itself on the path of data flow from source to destination. The attack is mainly dangerous in case of mission critical applications and has the potential to disrupt the normal network operation and render the network useless.

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.

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

II literature review

The Packet Droppers and Modifiers are common attacks in wireless sensor networks. It is very difficult to identify such attacks and this attack interrupts the communication in wireless multi hop sensor networks. We can identify the Packet Droppers and Packet Modifiers [2] using ranking algorithms and packet marks. A packet sender or forwarder adds a small number of extra bits, which is called packet marks. Node categorization algorithm to identify nodes that are droppers/modifiers for sure or are suspicious droppers/ modifiers. The different ranking algorithm can be used for detecting the packet dropping.

Global ranking

The Global ranking based approach is based on the heuristic method, the more times a node is identified as suspiciously bad, the more likely it is a bad node. The node with the highest value is chosen as a most likely bad node and all the pairs that contain this node are removed.

Stepwise ranking

Stepwise ranking based approach can be anticipated that the GR method will falsely accuse innocent nodes that frequently been parents or children of bad nodes. Once a bad node u is identified, for any other node v that has been suspected together with node u, the value of node v's accused account is reduced by the times that u and v have been suspected together.

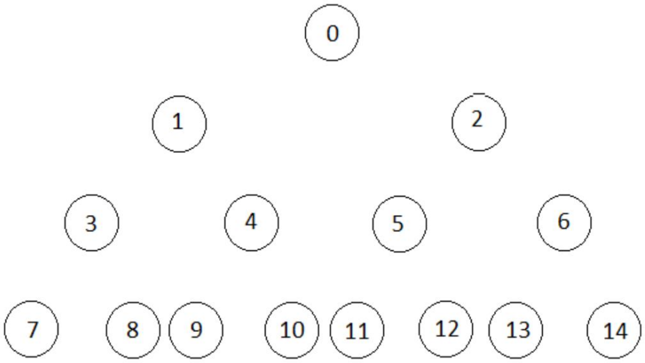
Hybrid Ranking

Hybrid Ranking Based (HR) approach has fever false accusations but may not detect as many bad nodes as the GR method. After a most likely bad node has been chosen, the one with the highest accused account value among the rest is chosen only if the node has not always been accused together with the bad nodes that have been identified. Modified packets will be detected by sink and it will be dropped and hence packet modifier can be identified as packet dropper .To enable en route detection of modifications, the afore described procedures for packet sending and forwarding can be slightly modified as follows. When a node u has a data item D to report, it can obtain endorsement message authentication codes (MACs) from its neighbors, which are denoted as MAC (D).

Detection of Packet Droppers in Wireless Sensor Networks Using Node Categorization Algorithm [3]. An intruder may launch some attacks due to packet dropping in order to disrupt the communication. To tolerate or mitigate such attacks, uses efficient technique to identifies the misbehaving forwarders that drop the packets. Tree on DAG (ToD) is a semi structured approach that uses Dynamic Forwarding on an implicitly constructed structure composed of multiple shortest path trees to support network scalability.

Tree on DAG

The key principle behind ToD is that adjacent nodes in a graph will have low stretch in one of these trees in ToD and thus resulting in early aggregation of packets. After performing local aggregation, all sensor nodes dynamically decide the forwarding path based on the location of the sources and aggregated packets are forwarded to the sink node on ToD. The sink node knows the ToD structure which shares a unique key with each node.



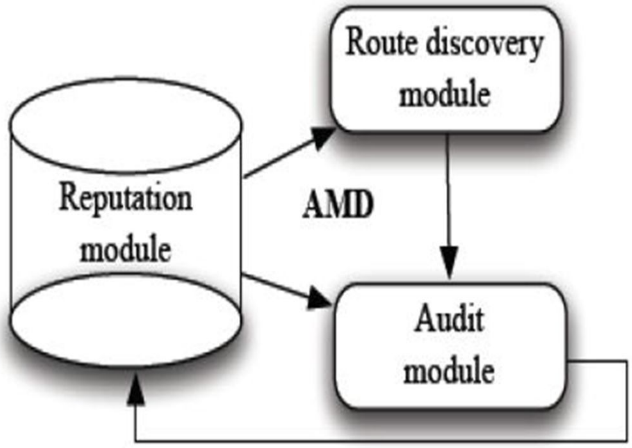
When a node wants to send out a packet, it attaches to the packet a sequence number, encrypts the packet only with the key shared with the sink, and then forwards the packet to its parent on the routing tree. When an innocent intermediate node receives a packet, it attaches a few bits to the packet to mark the forwarding path of the packet, encrypts the packet, and then forwards the packet to its parent. On the contrary, a misbehaving intermediate node may drop a packet it receives. On receiving a packet, the sink node decrypts it, and thus finds out the original sender and the packet sequence number. The sink node 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 node identifies packet droppers based Node Categorization Algorithm.

In the initialization phase, sensor nodes form a topology, which is a Tree on DAG (Directed Acyclic Graph). In each round, data is transferred through the routing tree to the sink node. Each packet sender/forwarder adds a small number of extra bits to the packet which is called packet mart. When one round is over, based on the packet mart carried in the received packets, the sink node runs a node categorization algorithm to identify nodes that are bad for sure (packet droppers), suspiciously bad (suspected to be packet droppers) and good for sure (no packet droppers). The routing tree is reshaped at every round. When certain number of rounds has passed, the sink node will have collected information about node behaviours in different routing topologies.

Detection and Isolation of Packet Droppers in Wireless Networks using Audit-based Misbehavior Detection [4]. Wireless ad hoc networks realize end-to-end communications in a cooperative manner. Multiple nodes coordinate to form a multi-hop route, when communication needs to take place between a source and a destination that are not within communication range. Thus, intermediate nodes are willing to carry traffic other than their own. For ad hoc networks deployed in hostile environments, a protocol compliant behavior on behalf of all nodes of the network cannot be assumed. Selfish and/or malicious users may misconfigure their devices to refuse forwarding any traffic, in order to conserve energy resources or degrade the network performance. so identifying and isolating misbehaving nodes that refuse to forward packets using Audit-based Misbehavior Detection(AMD).

Audit-based Misbehavior Detection

It effectively and efficiently isolates both continuous and selective packet droppers. AMD consists of three modules: the reputation module, the route discovery module, and the audit module. These modules are implemented in each node of the network and do not need any sort of centralized control. They closely interact to coordinate the functions of misbehavior detection, discovery of trustworthy routes, and evaluation of the reputation of peers.



The reputation module

The reputation module is responsible for managing reputation information. Every node of the network collects first-hand and second-hand reputation information for its peers.

The route discovery module

The route discovery module establishes a route between a source and a destination, using the reputation values computed by the reputation module.

The audit module

The audit module is responsible for detecting misbehaving nodes along entire paths from a source to a destination. The audit module operates on an end-to-end basis, thus allowing the concurrent behavior evaluation of all nodes along a particular path. The AMD system integrates reputation management, trustworthy route discovery, and identification of misbehaving nodes based on behavioral audits. All three modules are tightly integrated to ensure that multi-hop communications take place over paths free from malicious nodes.

Enhanced Detection of Packet Droppers and Modifiers using Node Categorization and Heuristic Ranking (NCHR) [5] is to identify compromised nodes and Secure Routing Encryption techniques are provided to ensure reliable communication. This effective scheme is used to catch both packet droppers and modifiers. In this scheme, first a routing tree is rooted at the sink. The sensor data are transmitted along the tree structure toward the sink, each packet sender or forwarder adds a small number of extra bits, which is called packet marks to the packet.

The format of the small packet marks is intentionally designed such that the sink can obtain very useful information from the marks. Specifically, based on the packet marks, the sink can figure out the dropping ratio associated with every sensor node. Every participating node computes two MACs over the event, one using its key shared with the Base Station, and the other using its pair wise key shared with its upper associated node. The node transmits the packet along with the MAC value produced and the forwarding node verifies the data integrity. The routing tree is reshaped and compromised nodes are identified using NHCH.

Node Categorization and Heuristic Ranking

In NHCH scheme packet droppers or modifiers are found by clustering the nodes depending on the risk factor and dropping ratio as good, moderate or bad. After finding, the nodes are further ranked to identify most nodes that are sure to drop packets. A routing table is maintained and an accused account is maintained using Ranking Technique in which nodes are ranked depending on their identification to be bad for several times. The most accused value node is fixed to be bad for sure. The accused value of nodes is reduced by the number of times it has been found together along with the bad node.

Then the sink runs node categorization algorithm to identify nodes that are droppers/modifiers for sure or are suspicious droppers/modifiers. As the tree structure dynamically changes every time interval, behaviours of sensor nodes can be observed in large variety of scenarios. Finally, as the information of node behavior's has been accumulated, the sink periodically runs the heuristic ranking algorithms to identify most likely bad nodes with small false positive. After finding out the compromised node secured routing path is found. A route request is broadcasted to all nodes which consist of a record listing the addressing of the intermediate nodes excluding the compromised nodes identified. Later shortest path is identified and data is transferred This scheme is effective in identifying both packet droppers and modifiers with low communication and energy overheads and being compatible with existing false packet filtering schemes, that can be deployed together with existing false packet filtering schemes is detected.

Many protocols for sensor network security provide confidentiality [6] for the content of messages and contextual information usually remains exposed. Such contextual information can be exploited by an adversary to derive sensitive information such as the locations of monitored objects and data sinks in the field. Attacks on these components can significantly undermine any network application. It formalizes the location privacy issues in sensor networks under this strong adversary model and computes a lower bound on the communication overhead needed for achieving a given level of location privacy. Catching Moles and Packet Droppers can be managed based on two techniques. Source location privacy- periodic collection and source simulation. Sink location privacy-– sink simulation and backbone flooding.

Homomorphic Encryption (HE)

Hemomorphic Encryption is used on the Encoding Vector to achieve the efficient privacy in WSNs. With the use of HEs the confidentiality of the Encoding Vector is effectively guaranteed making it almost complicated for an adversary to obtain the plaintext. Instead of Link-to-Link encryption, End-to-End encryption on Encoding Vectoris employed to achieve even energy efficiency and avoiding intermediate coding/mixing operations. The secure communication methods that preserve the privacy against both global and local eavesdropper.

Node Categorization and Ranking

Node Categorization and Ranking will be performed based on the node behavior. If there is any modification or drop of packets in node it assumes negative value for modifier or dropper. Sink performs Ranking for each node based on the Category of nodes. Sink gives ranking like Good, Temporarily Good, Suspiciously Bad, Bad based on the node behavior in the process.

Eavesdropper

The global eavesdropper who can visualize the entire network and can monitor the traffic traversing the network and applying network coding mechanism by tagging the packets with the Encoding Vector. Source imitation approach can find out the number of candidate traces present in the network and evaluate the Hemimorphic Encryption for location privacy in sensor networks. Compute the optimal path between the source and destination to maintain the energy reserve in the sensor network

Sender Node

Sender selects the file which is to present. And then it split into the number of packets based on the size for adding some bits in it. And then it encrypts all the splitted packets. Sender adds some bits to each encrypted packets before sending that. Bit Addition for each packet is identification for sender. After adding of bits to each packet, it sends the packets to the nearest node or intermediate node. The intermediate node receives Packets from the sender. After receiving all packets from sender, it encrypts all packets again for authentication. Before sending to sink, intermediate add some bits to each packet for node identification. After adding some bits from intermediate, it sends all packets to the sink. Before sending all packets to sink, packets dropping or packets modifying may be occur in intermediate.

Sink

Sink receives all packets from the sender node, and it verifies all packets which are dropped or not. And it also verifies the packets which are modified or not and it can identify the modifiers in the process based on the bit identification. After receiving all packets in sink, it decrypts all packets. After the decryption if there is no modified or dropped packets, it merge all packets. After merging, Sink can receive the original file.

Conclusion

The effective schemes are used to identify misbehaving forwarders that drop or modify packets. Each packet is encrypted and padded so as to hide the source of the packet. The packet mark, a small number of extra bits, is added in each packet such that the sink can recover the source of the packet 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 detection algorithm can achieve a high detection accuracy and a low false alarm rate as indicated by the extensive literature study. The nice feature of the algorithm is that it requires no prior knowledge about normal or malicious sensors, which is important considering the dynamic attacking behaviors. Further, our algorithm can be employed to inspect any aspects of networking activities, with the multiple attributes evaluated simultaneously. The algorithm is pure localized, thus scales well to large sensor networks. We notice that the detection algorithm can be specialized by exploring the degree of the correlations existent among different aspects of sensor networking behaviors.

Reference

[1] Bhargavi Singh, “Security Mechanisms for Selective Forwarding Attack in Wireless Sensor Networks: Review and Analysis”, IOSR Journal of Computer Engineering (IOSR-JCE) e-ISSN: 2278-0661, p-ISSN: 2278-8727, Volume 16, Issue 4, PP. 07-13, August 2014.

[2] B.Kishore Kumar, G.K.Venkata Narasimha Reddy, “Identification of Packet Dropping and Modification in Wireless Sensor Networks”, International Journal of Computational Engineering Research, Volume 03, Issue 7, 2013.

[3] N.Vanitha, G.Jenifa, “Detection of Packet Droppers in Wireless Sensor Networks Using Node Categorization Algorithm”, International Journal of Advanced Research in Computer Science and Software Engineering, ISSN: 2277 128X, Volume 3, Issue 3, March 2013.

[4] Dr.K.Kungumaraj, J.Vijayabharathi, “Detection and Isolation of Packet Droppers in Wireless Networks”, International Journal of Engineering and Computer Science, ISSN: 2319-7242, Volume 3 Issue 8 PP. 7571-7577, August 2014.

[5] R. Karthikeyan, “Enhanced Detection of Packet Droppers and Modifiers in Wireless Sensor Networks”, International Journal of Innovative Research in Computer and Communication Engineering (An ISO 3297: 2007 Certified Organization) Volume 2, Issue 1, March 2014.

[6] Mohammed Hajee, Mohammed Abdul Rawoof, “Catching Moles and Packet Droppers in Wireless Sensors Network”, International Journal of Science and Research (IJSR), Volume 3, Issue 9, September (2014).

[7] V.Redya Jadav, A.Mothilal, N.Srikanth, “In Wireless Sensor Networks Catching Packet Droppers and Modifiers”, International Journal of Research and Computational Technology, ISSN: 0975-5665, Vol.5 Issue.2, May 2013.

[8] E.Surya Praba, k.Sivan Arul Selvan, “Identification of Packet Droppers and Modifiers in Wireless Sensor Networks”, International Journal of Societal Applications of Computer Science Volume 2, Issue 1,ISSN 2319 – 8443, January 2013.

[9] Gaurav, Naresh Sharma, Himanshu Tyagi, “An Approach: False Node Detection Algorithm in Cluster Based MANET”, International Journal of Advanced Research in Computer Science and Software Engineering, Volume 4, Issue 2, February 2014.

[10] PrasenjitChanak,TuhinaSamanta,Indrajit Banerjee, “A Survey on Energy Efficiency Problem in Wireless Sensor Networks”, International Journal of Advanced Research in Computer Science and Software Engineering, Volume 4, Issue 3, March 2014 ISSN: 2277 128X

[11] Latha Venkatesan1, S. Shanmugavel, "A Survey on Modeling and Enhancing Reliability of Wireless Sensor Network", Wireless Sensor Network, 2013, 5, 41-51**,** http://dx.doi.org/10.4236/wsn.2013.53006 Published Online March 2013.

[12] Priya Gopi, "Multipath Routing in Wireless Sensor Networks: A Survey and Analysis", IOSR Journal of Computer Engineering (IOSR-JCE) e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 16, Issue 4, Ver. VI (Jul – Aug. 2014), PP 27-34 www.iosrjournals.org.

[13] S.Lavanya, Dr. S.Prakasm, "Reliable Techniques for Data Transfer in Wireless Sensor Networks", International Journal Of Engineering And Computer Science ISSN:2319-7242 Volume 3 Issue 12 December 2014, Page No.9726-9731.

[14] Apoorva M ,Hemanth S R, "Multipath Routing In Wireless Sensor Networks: A Survey and Energy Consumption Analysis" International Journal For Technological Research In Engineering Volume 1, Issue 1 2, ISSN (Online): 2347-4718 August- 2014.

[15] Aayushi Mahajan, Suhaib Ahmed, "Comparative Analysis of Different Data Dissemination Strategies in Wireless Sensor Networks", International Journal of Advanced Research in Computer and Communication Engineering Vol. 3, Issue 4, ISSN (Online) : 2278-1021 April 2014.