

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 2, February 2019

Catching Packet Droppers and Modifiers in Wireless Sensor Network

Raghuram A.S¹

Asst. Professor, Dept. of CSE, ATMECE, MYSORE, India¹

ABSTRACT: In a wireless sensor network, sensor nodes monitor the environment, detect events of interest, produce data and collaborate in forwarding the data toward a sink. Because of the ease of deployment, the low cost of sensor nodes and the capability of self-organization, a sensor network is often deployed in an unattended and hostile environment to perform the monitoring and data collection tasks. When it is deployed in such an environment, it lacks physical protection and is subject to node compromise. After compromising one or multiple sensor nodes, an adversary may launch various attacks to disrupt the in-network communication. Among these attacks, two common ones are dropping packets and modifying packets, i.e., compromised nodes drop or modify the packets that they are supposed to forward. Packet dropping and modification are common attacks that can be launched by an adversary to disrupt communication in wireless multi hop sensor networks. Many schemes have been proposed to mitigate or tolerate such attacks, but very few can effectively and efficiently identify the intruders. To address this problem, propose a simple yet effective scheme, which can identify misbehaving forwarders that drop or modify packets. These countermeasures 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. Propose a simple yet effective scheme to catch both packet droppers and 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.

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

I. INTRODUCTION

In computer networking, a **packet drop attack** or **black hole attack** is a type of denial-of-service attack in which a router that is supposed to relay packets instead discards them. This usually occurs from a router becoming compromised from a number of different causes.

A **wireless sensor network (WSN)** of spatially distributed autonomous sensors to monitor physical or environmental conditions, such as temperature, sound, pressure, etc. and to cooperatively pass their data through the network to a main location. The more modern networks are bi-directional, also enabling control of sensor activity. The development of wireless sensor networks was motivated by military applications such as battlefield surveillance; today such networks are used in many industrial and consumer applications, such as industrial process monitoring and control, machine health monitoring, and so on. In network there two common attacks are *packet dropping* and *modifying packets*

II. RELATED WORKS

The approaches for detecting packet dropping attacks can be categorized as three classes: multipath forwarding approach, neighbour monitoring approach, and acknowledgment approach. Multipath forwarding [3], [1] is a widely adopted countermeasure to mitigate packet droppers, which is based on delivering redundant packets along multiple paths. Another approach is to exploit the monitoring mechanism [4], [8]. The watchdog method was originally proposed to mitigate routing misbehaviour in mobile ad hoc networks [3]. It is then adopted to identify packet droppers in wireless sensor network [9], [10]. When the watchdog mechanism is deployed, each node monitors its

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 2, February 2019

neighbourhood promiscuously to collect the firsthand information on its neighbour nodes. A variety of reputation systems have been designed by exchanging each node's firsthand observations, which are further used to quantify node's reputation. Based on the monitoring mechanism, the intrusion detection systems are proposed in [3] and [4]. However, the watchdog method requires nodes to buffer

The packets and operate in the promiscuous mode, the storage overhead and energy consumption may not be affordable for sensor nodes. In addition, this mechanism relies on the bidirectional communication links; it may not be effective when directional antennas are used [5]. Particularly, this approach cannot be applied when a node does not know the expected output of its next hop since the node has no way to find a match for buffered packets and overheard packets. Note that, this scenario is not rare, for example, the packets may be processed, and then encrypted by the next hop node in many applications that security is required. Since the watchdog is a critical component of reputation systems, the limitations of the watchdog mechanism can also limit the reputation system. Besides, a reputation system itself may become the attacking target. It may either be vulnerable to bad mouthing attack or false praise attack [2]. The third approach to deal with packet dropping attack is the multihop acknowledgment technique [1], [2], [4],[9]. By obtaining responses from intermediate nodes, alarms, and detection of selective forwarding attacks can be conducted. To deal with packet modifiers, most of existing countermeasures [6], [7], [8], [9] are to filter modified messages within a certain number of hops so that energy will not be wasted to transmit modified messages. The effectiveness to detect malicious packet droppers and modifiers is limited without identifying them and excluding them from the network. Researchers hence have proposed schemes to localize and identify packet droppers; one approach is the acknowledgment-based scheme [3], [6] for identifying the problematic communication links. It can deterministically localize links of malicious nodes if every node reports ACK using onion report. However, this incurs large communication and storage overhead for sensor networks. The probabilistic ACK approaches are then proposed in [3] and [10], packet modifiers. This degrades the efficiency of deploying the PAA scheme.

III. METHODOLOGY

To catch both packet droppers and modifiers. In this scheme, a routing tree rooted at the sink is first established. When 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 deliberately designed such that the sink can obtain very useful information from the marks. Based on the packet marks, the sink can figure out the dropping ratio associated with every sensor node, and then runs algorithm to identify nodes that are droppers/modifiers for sure or are suspicious droppers/modifiers. As the tree structure dynamically changes every time interval, behaviors of sensor nodes can be observed in a large variety of scenarios. As the information of node behaviors has been accumulated, the sink periodically runs our proposed heuristic ranking algorithms to identify most likely bad nodes from suspiciously bad nodes.

When compare them with other caching schemes, showing that our solution succeeds in creating the desired content diversity, thus leading to a resource-efficient information access. Simulate caching algorithms in different ad hoc network scenarios and Data caching strategy for ad hoc networks whose nodes exchange information items in a peer-to-peer fashion. These decisions are made depending on the perceived "presence" of the content in the nodes proximity, whose estimation does not cause any additional overhead to the information sharing system. However, the solution that was proposed is based on the formation of an overlay network composed of "mediator" nodes, and it is only fitted to static connected networks with stable links among nodes. We proposed to mitigate or tolerate such attacks, but very few can effectively and efficiently identify the intruders. To address this problem, we propose a simple yet effective scheme, which can identify misbehaving forwarders that drop or modify packets. Extensive analysis and simulations have been conducted to verify the effectiveness and efficiency of the scheme.

MODULES

In our system we define 9 modules which are performed by sensor node, sink node and router. They are:

- Broadcast route request packet from source node.

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 2, February 2019

- Calculating shortest path from source node to sinknode.
- Generate and distributing sequence keys at sinknode.
- Reading temperature from temperaturesensor.
- Encryption and Decryption using Rijndael algorithm.
- Keep sending temperature from sensor node through shortestpath.
- Identifymodifier.
- Identfydropper.
- Changingroute.

AODV

Ad-hoc On-demand Distance Vector (AODV) routing protocol, AODV is an „on demand routing protocol“ with small delay. That means that routes are only established. When needed to reduce traffic overhead. AODV supports Unicast, Broadcast and Multicast without any further protocols. The Count-To-Infinity and loop problem is solved with sequence numbers and the registration of the costs. Ad hoc On-demand Distance Vector Routing (AODV) is an improvement on the DSDV algorithm. AODV minimizes the number of broadcasts by creating routes on-demand as opposed to DSDV that maintains the list of all the routes. To find a path to the destination, the source broadcasts a route request packet. The neighbors in turn broadcast the packet to their neighbors till it reaches an intermediate node that has recent route information about the destination or till it reaches the destination (a). A node discards a route request packet that it has already seen. The route request packet uses sequence numbers to ensure that the routes are loop free and to make sure that if the intermediate nodes reply to route requests, they reply with the latest information only. When a node forwards a route request packet to its neighbors, it also records in its tables the node from which the first copy of the request came. This information is used to construct the reverse path for the route reply packet. AODV uses only symmetric links because the route reply packet follows the reverse path of route request packet. As the route reply packet traverses back to the source (b), the nodes along the path enter the forward route into their tables. If the source moves then it can reinitiate route discovery to the destination. If one of the intermediate nodes moves then they moved nodes neighbor realizes the link failure and sends a link failure notification to its upstream neighbors and so on till it reaches the source upon which the source can reinitiate route discovery if needed.

RIJNDAEL ALGORITHM

In proposed scheme for packet encryption and decryption. Rijndael Algorithm the block cipher algorithm recently chosen by the National Institute of Science and Technology (NIST) as the Advanced Encryption Standard (AES). It supersedes the Data Encryption Standard (DES). Like DES, it is a block cipher. It uses 128-bit, 192-bit or 256-bit keys. This implementation encrypts 128-bit blocks. (DES used 56-bit keys and 64-bit blocks.) NIST selected Rijndael as the standard symmetric key encryption algorithm to be used to encrypt sensitive (unclassified) American federal information. The choice was based on a careful and comprehensive analysis of the security and efficiency characteristics of Rijndael's algorithm. Rijndael is an iterated block cipher. Therefore, the encryption or decryption of a block of data is accomplished by the iteration (a round) of a specific transformation (a round function). Rijndael also defines a method to generate a series of sub keys from the original key. The generated sub keys are used as input with the round function. Rijndael was developed by Belgian cryptographers Joan Daemen of Proton World International and Vincent Rijmen of Katholieke University Leuven. The algorithm that they developed was designed as an easily understandable mathematical structure that can be broken down into simple components. Rijndael was evaluated based on its security, its cost and its algorithm and implementation characteristics. The primary focus of the analysis was on the cipher's security, but the choice of Rijndael was based on its simple algorithm and implementation characteristics. There were several candidate algorithms but Rijndael was selected because based on the analyses, it had the best combination of security, performance, efficiency, ease of implementation and flexibility.

Many cryptographic algorithms exist to address and attempt to solve the issue of information security. Many of these algorithms were candidates for the AES. NIST selected the AES based on its uncontested ability to provide good security. Though good security was the primary quality required of the winning formula, factors such as speed and versatility across a variety of computer platforms also were considered. In other words, the algorithms must be

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 2, February 2019

able to run securely and efficiently on large computers, desktop computers and even small devices such as smartcards. The candidates' security was analysed with respect to their ability to resist cryptanalysis, the soundness of algorithms' mathematical basis and the randomness of the output. The characteristics of the algorithms were analysed for flexibility, hardware and software suitability and simplicity. Cost was also important based on speed and the cost of hardware implementations.

RANKING-BASED APPROACH

Step 1: the number of packets passed through the particular node.

Step 2: sink node check the rank of each node. Step 3: highest rank is first added to the list Step 4: goto step 3 until reach sink node.

Step 5: take difference between each node.

Step 6: node which is having less rank consider as dropper node.

Step 7: stop.

PACKET DROPPING

Consider a scenario of a network with four sensor nodes where in one each is source and sink and rest are the intermediate nodes. The sensor in the source senses the packet arrival and broadcast the request packet to all of the neighbouring nodes to find the best path to the destination. To avoid receipt of the same broadcast packets, the node blocks the same packets which are being sent by the same IP address.

The source finds out the best path to send the packets to the destination using adaptive routing strategies. The source starts transmitting the packets to the next immediate node in the path established. Each node will have a log table to keep track of the number of packets received from the predecessor node. If the packets arrival time at the destination exceeds the stipulated time of the transmission, the destination suspects the behavior of the intermediate nodes to be malicious, it then sends an analyzer program to every node in the reverse order of the packet transmit. On reaching the intermediate node the analyzer program will check the log table of the node and extracts the information about the number of packets forwarded by that node. The analyzer program calculates the dropping ratio, which gives the exact number of packets the node actually dropped. The analyzer program compares the dropping ratio of each intermediate node and notifies the destination about the node which has dropped maximum number of packets. Now the destination block lists the malicious node for future transmissions.

PACKET MODIFICATION

Consider a scenario of a network with four sensor nodes where in one each is source and sink and rest are the intermediate nodes. The sensor in the source senses the packet arrival and broadcast the request packet to all of the neighboring nodes to find the best path to the destination. To avoid receipt of the same broadcast packets, the node blocks the same packets which are being sent by the same IP address. The source finds out the best path to send the packets to the destination using adaptive routing strategies. The sink distributes the key to the nodes found on the defined path. It also holds the keys that are distributed to the intermediate nodes. Now the source encrypts the packet to be transmitted using the key that is shared only between the sink and itself. The intermediate node encrypts the packets using shared key which are received from the predecessor node and forwards the packet to the next node on the path. Sink will decrypts the received packet using the shared key. We assume that packet has been modified in an intermediate node, which drops the received packet and modifies it using shared key and transmit the packet. While decrypting the packet, destination notices that the packet cannot be decrypted since the modified packet was not encrypted by the predecessor node using the key that is been distributed Destination will block list the node that modified the packet for future transmission.

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 2, February 2019

IV. EXPERIMENT RESULTS

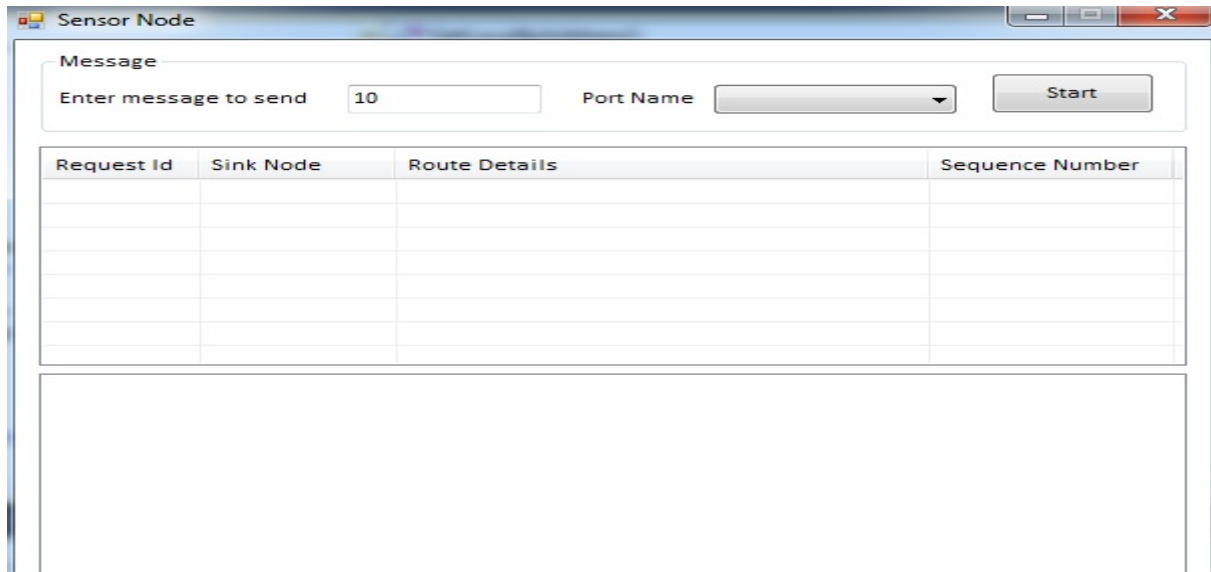


Figure 1: Source node sends the data to the destination nodes via router or intermediate nodes

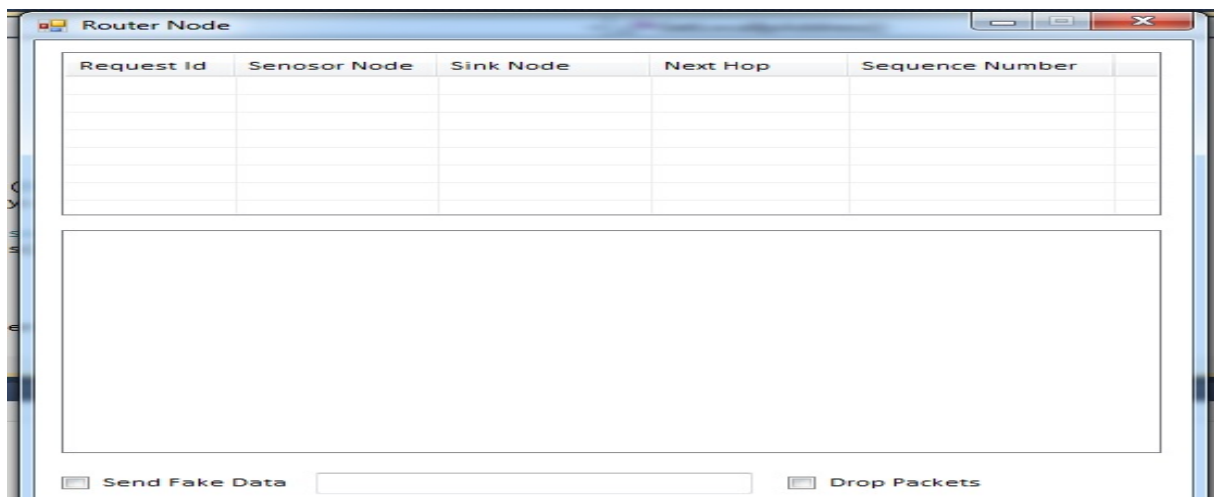


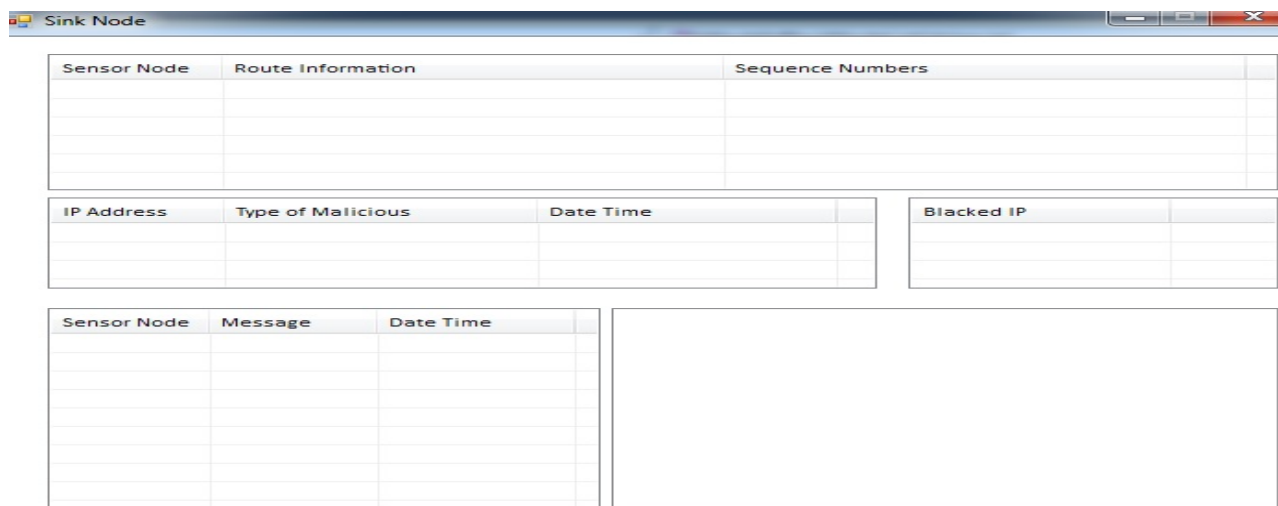
Figure 2: Router nodes that transfers the data to the next node

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 2, February 2019



Sensor Node	Route Information	Sequence Numbers

IP Address	Type of Malicious	Date Time

Blacked IP

Sensor Node	Message	Date Time

Figure 3: Sink nodes that receives the data from the source node through router node

V. CONCLUSION

We propose a simple yet effective scheme 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 our heuristic ranking algorithms with small false positive. Extensive analysis, simulations, and implementation have been conducted and verified the effectiveness of the proposed scheme.

REFERENCES

1. Chris Karlof, David Wagner, "Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures" Computer, vol. 36, no. 10, pp. 103-105, Oct.2003.
2. S. Sajithabanu, M. Durairaj, "Detecting False Data in Wireless Sensor Network using Efficient Becan Scheme" International Journal of Computer Applications (0975 – 8887) Volume 43– No.18, April2012.
3. Kejun Liu, Jing Deng, Pramod K. Varshney, and KashyapBalakrishnan,"An Acknowledgment-Based Approach for the Detection of Routing MisbehaviourinMANETs"IEEETransactionson Mobile Computing, vol. 6, no. 5, pp. 536-550, May 2007.
4. WazirZadaKhana, Yang Xiangb, Mohammed Y Aalsalema, QuratulainArshada,"The Selective Forwarding Attack in Sensor Networks: Detections and Countermeasures" vol .2, no. 12,pp. 33-44, April2012.
5. R.MohanaSundari, Mrs.P.R.Vijayalakshmi "Secure and Data Aggregation in Wireless Sensor Networks" International Journal of Advanced Engineering Applications, Vol.4, Iss.1, pp.32-36 (2011).
6. Yih-Chun Hu a, David B. Johnson b, Adrian Perrig, "SEAD: secure efficient distance vector routing for mobile wireless ad hoc networks" vol. 1, no. 18, pp. 175–192,(2003).
7. Sencunzhu, sanjeevsetia, sushiljajodia, pengning, "Interleaved hop-by-hop authentication against false data injection attacks in sensor networks" IEEE Symp. Security and Privacy,2004.
8. Fan Ye, HaiyunLuo, Songwu Lu, Member, IEEE, and Lixia Zhang, Senior Member, IEEE. "Statistical en-route filtering of injected false data in sensor networks" IEEE journal on selected areas in communications, vol. 23, no. 4, April2005.
9. Xin Zhang, Abhishek Jain, Adrian Perrig, " Packet-dropping Adversary Identification for Data Plane Security"vol.5,no. 9-12, December2008.
10. Rosa Mavropodi , Panayiotis Kotzanikolaou, Christos Douligeris, " SecMR – a secure multipath routing protocol for ad hoc networks" science direct, Ad Hoc Networks 5 (2007)87–99.
11. Rajkumar Singh, "Ad hoc On-demand Distance Vector" (2012),PP.1-19.
12. VikasKawadia, Binita Gupta, "System Services for Ad-Hoc Routing: Architecture, Implementation and Experiences" (2012) pp1-5.
13. C. Sanchez-Avila, R. Sanchez-Reillot "The Rijndael Block Cipher"(2011).pp.1-12.