ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 2, February 2016

Density Network Attack Detection based on Signature in Wireless Network Sensor Systems

Prakash M[1] ,Shalomi Junofia R[2]

M.E. Student, Dept. of CSE., Valliammai Engineering College, Kanchipuram, India[1,2]

ABSTRACT: Wireless Sensor Network Coding Systems have a vital role in the areas such as military applications,environmentalmonitoring,health care ,home or industrial automation,etc., Thus the Wireless Sensor Network always have the disadvantages of low battery life,low processing power,smallmemory,deployment in hostile environment. Thus an effective detection mechanism is needed to prevent Wireless Sensor Network Systems. We propose, a signature based detection for wormhole attack inside the Sensor Network. Each attack has a certain signature, based on these rules are detection of different types of attack inside the Wireless Sensor Network .This signature based approach will identify attacks such as wormhole, black hole and Sybil attack . Thus the proposed system also improves the reliability of data by measuring the parameters such as throughput and packet delivery ratio while detecting of the routing attacks

KEYWORDS: Wireless Sensor Networks; signature; rule based ;throughput; packet delivery ratio.

I. INTRODUCTION

WSN consists of spatially distributed sensor devices which monitor physical environment conditions[1] which employ a multi-hop information without a proper infrastructure due to their deployment nature. These networks are vulnerable to security threats, which includes low battery life ,low processing power ,small memory, deployment in hostile environment and the radio links are also insecure[2].An effective detection mechanism to prevent WSN for a reliable transmission.Researchers often do not focus on security aspects while designing a new routing protocol[3]. Attacks are classified into internal and external. Evesdropping and injecting fault which causes Denial of Service(DoS) are external attacks. Internal attacks are caused by one of the nodes in sensor network. As there is no standard layered architecture of the communication protocol for wireless sensor network,every layer can be attacked due to their loophole nature. Routing attacks are vulnerable as they deal with Data Integrity[4,5].

To protect from attacks, a security framework should be designed. Cryptographic techniques and authentication are used to defend external attacks. The area of deployment is not physically protected and an attacker can easily access the node and capture some nodes. The software running nodes are tamper resistant and hence can be modified by a variety of internal attacks. Detection based techniques implemented so far can isolate attacker after prevention based techniques fail and inside attacks are not detected[6]. Signature based approach also called specification based scheme and which is suitable for WSN in account of simple implementation and high detection rate.

This paper proposes the signature based routing attacks detection system, which secures wireless sensor networks from routing attacks. The aim of this work is to design and implement the routing attacks for WSNs.The proposed system includes three modules information gathering – which is used to collect data from neighbour nodes and filters the features; decision making-used to apply rules on the filtered data;attack detection- which compares the failure counter value with the threshold value.The attack is detected according to the above mentioned features.

II. RELATED WORK

The wormhole attack can be detected by an independent physical metric such as time delay. A packet leashed is technique is proposed in [10] that prevent packets from trav-elling farther than radio transmission range. The drawback of this scheme is that each node must know its own location. So, packet leashes have limited applicability in wireless sensor networks.Location–Aware ‘Guard’ Nodes (LAGNs) technique is proposed in [11] to prevent the wormhole attack on wireless ad hoc networks, in which the guard node is used to detect the message flow between nodes. The main drawback of this scheme is that the guard nodes are needed to know their own location and it is suitable for stationary

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 2, February 2016

sensor networks.The distributed detection method proposed in [12] which rely solely on network con-nectivity information. It detects the wormhole based on topology. Tun et al. [13] proposed round trip time and neighbor numbers based wormhole detection. Detection rate depends up on the wormhole length. Bandwidth overhead and memory overhead incurred after the deployment.Newsome et al. [14] proposed several methods for detecting Sybil entities in a sensor network. The proposed detection technique requires the engagement of all neighboring nodes by inquiring them to respond to queries on specified channels or to carry pre distributed keys. This approach is suitable stationary sensor networks only. Sharmila et al. [15] proposed Sybil attack detection technique, which allows an identity to remain identical from other nodes in the group of mobile nodes. An attacker who wishes to influence the identity can be easily found by group head by checking the hop distance and node identity. The main drawback of this system is centralized. Tamilselven et al. [16] proposed an enhancement of AODV protocol which avoided black-hole attacks through the use of collective route reply table. Scalability is main drawback of this mechanism.Zhao et al. [17] proposed a statistical Analysis and Time Constraint Algorithm for Split Multi-path Routing Protocol (SMR). The algorithm identifies the Wormhole attack when only there is a dramatic change in statistics of routing information stored in the Sink Node.

III. PROPOSED ALGORITHM

A. *Signature Based Approach:*

Signature Based Approach consists of three modules

- Information gathering
- Decision Making
- Attack Detection.

B. *Description of the Proposed System:*

The description of the signature based approach is explained by the following diagram done by three phases

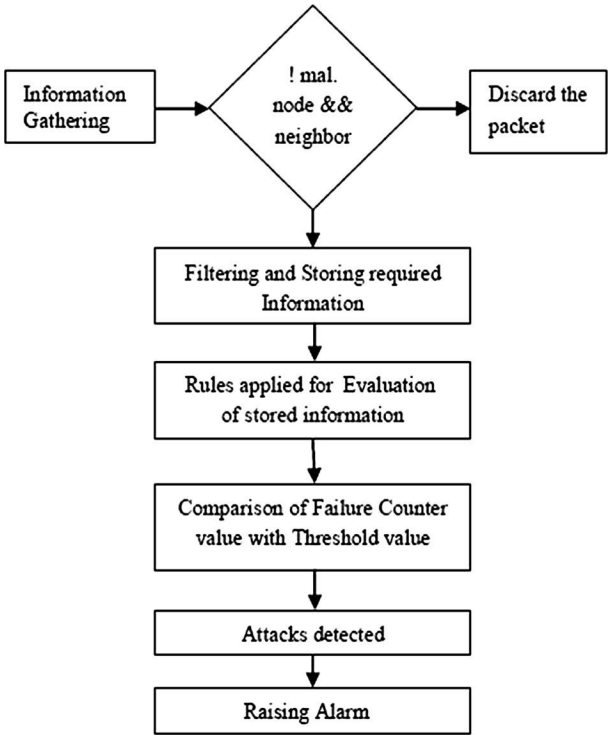

Fig.1.Different phases of attack detection

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 2, February 2016

Phase 1:Information gathering:

Whenever a node receives a message , this phase validates whether it is a neighbouring node or not[3]. If the sender node is a legitimate node then it performs the necessary action otherwise it discards it.Then the important information are stored for a subsequent analysis.

Phase 2:Decision Making:

It finds the adversary nodes.The stored node is evaluated according to the sequence of specified rules. To detect attack specified rules are implied.If a failure of a message occurs, failure counter is incremented then the message will be discarded and no other rules can be applied to it.

Phase 3:Attack Detection:

The detection is done by means of threshold values which is set after a normal analysis of the network and the specific attacks are launched based on the values. If the value of the attacker node overcomes the threshold value then a particular attack will be detected. In this system, the following routing attacks are considered:

1.Sybil attack:

In a Sybil attack, an attacker can appear to be in multiple places at the same time. This can be convincing by creating fake identities of nodes located at the edge of communication range.

2.Wormhole attack:

In this attack an adversary could convince nodes who would normally be multiple hops from a base station that they are only one or two hops away via the wormhole. The simplest case of this attack is to have a malicious node forwarding data between two legitimate nodes. Wormholes often convince distant nodes that they are neighbors, leading to quick exhaustion of their energy resources. An adversary situated close to a base placed wormhole.

3.Black-hole attack:

The black hole attack positions a node in range of the sink and attracts the entire traffic to be routed through it by advertising itself as the shortest route. The adversary drops packets coming from specific sources in the network. This attack can isolate certain nodes from the base station and creates a discontinuity in network connectivity.

C.*Rules association with attacks:*

we describe the network features considered and the associated attacks and rules. Many nodes have to retransmit the message and if this node is tampered, it can perform the selective forwarding and black hole attacks. Here we use the retransmission rule. The data message comprises the sensor reading. Since we do not have any kind of data fusion or aggregation, the message received by the common node has to be trans-mitted with no payload alteration. We can detect the intruder that modifies the message using the integrity rule. A node can only receive messages from neighbors. The radio range rule can detect the wormhole and hello flood attacks. Each node has its identity in way of physical identity and MAC identity. The physical identities can be convinced by creating fake identities of nodes located at the edge of communication range. But the MAC identity of a node would not change for any circumstances. So this rule can be used to detect the Sybil attack in the network.

IV. IMPLEMENTATION

We have developed our own WSN simulator. This simulator has been implemented in NS 2. We have implemented a discrete event model, in which the analysis nodes keep their states during the simulation until the occurrence of some event such as receiving or sending a message, the occurrence of sensor and the activation of an attack. Network sensor events are generated randomly and nodes are not synchronized, as an attempt to approximate the simulator to the behavior of a real network. Our simulator is composed of the following elements: network, message, sensor node, intruder node, base station, events and attacks, detector node. The network module is responsible for the message exchange between the elements in such way that it can simulate the functioning of a real WSN. The sensor node has

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 2, February 2016

sensor and router functions. As a sensor, it collects sensor data, and sends it to the base station. As a router, it retransmits all messages directed to the base station.

Every sensor node is responsible for monitoring its neighbors looking for intruders. By doing this, the node keeps its radio in a promiscuous mode, storing relevant information and processing it according to selected rules. This node also executes the sensor/router functions since it is a common node where the detection system was installed. The intruder node switches between a common node behavior and an intruder behavior. The intruder behavior depends on the considered attack. The intruder can spend its whole time for performing an attack. In the context of these experiments the base station is only the destination of all data messages. Only attacks over data messages were taken into account.

The data message considered here has the following fields: next hop, message type, previous hop, origin, final destination, sequence number, and data. We have simulated a plan and fixed network with random node distribution. If the number of nodes getting increased in the sensor network, individual nodes are uniquely identified and have a fixed radio range because the simulated network is dynamic. Each node has to route the sensed data towards the base station. Because of the insecurity in radio links the WSN may vulnerable to different routing attacks.

We have simulated a network comprised of 50 nodes randomly distributed. The goal of our experiments is to evaluate the proposed detection system in particular, the amount of raised detections and false positives. In which, few nodes are selected and provided with attack behaviour.

The network showed in Fig. 1 is able to transmit 22 packets if total transmission energy metric is used and 17 packets if used maximum number of hops metric. And the network lifetime is also more for total transmission energy. It clearly shows in Fig. 2 that the metric total transmission energy consumes less energy than maximum number of hops. As the network is MANET means nodes are mobile and they change their locations. After nodes have changed their location the new topology is shown in Fig .3 and energy consumption of each node is shown in Fig. 4. Our results shows that the metric total transmission energy performs better than the maximum number of hops in terms of network lifetime, energy consumption and total number of packets transmitted through the network.

V.**Results and Discussions**

In this simulation, the detection system performance is measured by comparing the throughput and packet delivery ratio of the network before and after detecting the attack

A.*Throughput and Packet Delivery Ratio*

The throughput is the average rate of successful message delivery over a communication channel. The throughput is measured in kilo bits per second (kbps or kbit/s). The number of packets sent and throughput vary due to the presence of malicious nodes. A node illegiti-mately claims multiple identities or claims fake IDs, the WSN suffers from an attack called sybil attack. black hole detection. The packet delivery ratio is gradually increases when time increases compared to packet delivery ratio of without worm hole detection.

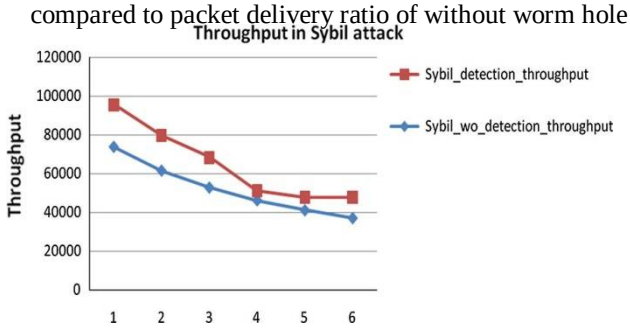

Fig.2.throughput in sybil attack

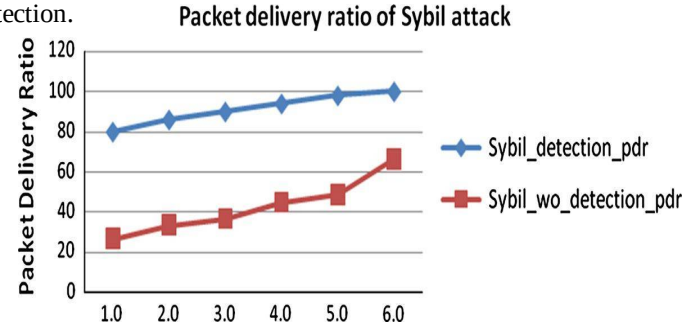

Fig. 3. Packet delivery ratio in Sybil attack

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 2, February 2016

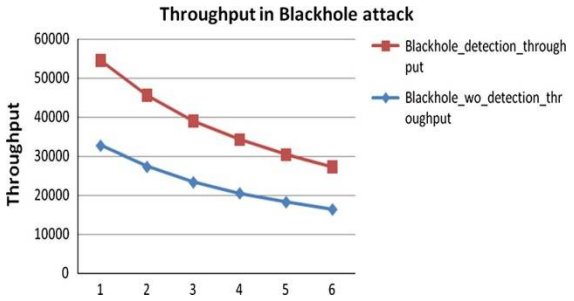

Fig. 4. Throughput in blackhole attack

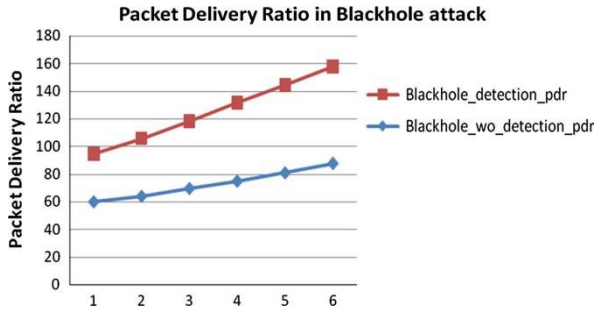

Fig 5. Packet delivery ratio in blackhole attack

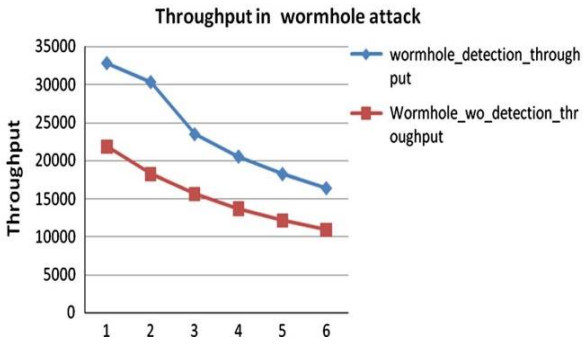

Fig 6.Throughput in Wormhole attack

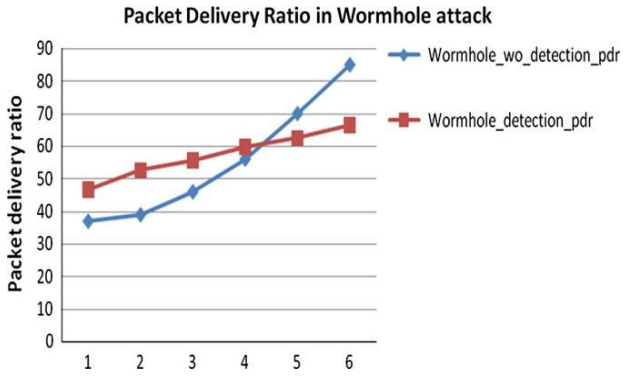

Fig 7.Packet delivery ratio in Wormhole attack

The Figs. 2 and 3shows the throughput and packet delivery ratio of sybil attack. After detection it can be observed that the packet delivery ratio and throughput has improved in the network. Greater the value of throughput means better the performance of the protocol.

The throughput and Packet delivery ratio of the black hole attack is shown in Figs. 4 and 5 respectively. The Fig. 4 shows the throughput of the WSN after black hole detection is comparatively higher than throughput of network without black hole detection. The packet delivery ratio also increased after detecting the black hole attack.

The throughput and Packet delivery ratio of the worm hole attack is shown in Figs. 6 and 7 respectively. The Fig. 6 shows throughput of the WSN after worm hole detection is comparatively higher than throughput of network without others.

V. CONCLUSION AND FUTURE WORK

Secure routing is the critical issue in the case of wireless sensor networks due to its poor resource constraints and emerging new unknown attacks. The routing protocols are designed without considering security as main fact while transmitting the data in WSN. Hence, it is necessary to frame a security framework that makes the WSN resilient against routing attacks. The aim of this work is to design and implement the routing attacks detection approach for WSNs. In particular, we briefly looked into black hole, wormhole and Sybil attacks. The proposed approach proves that the routing attacks have been detected and the data has been reliably transferred. Then, considered parameter values such as throughput and packet delivery ratio have been increased, Hence, the empirical results show that the performance of network has been improved.

In future, an intrusion detection system will be developed for detecting unknown routing attacks using fuzzy logic systems, because the signature based detection system is developed only for known attacks.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 2, February 2016

REFERENCES

1. Akyildiz, I. F., Su, W., Sankarasubramaniam, Y., &Cayirci, E. (2002). Wireless sensor networks: a survey. Computer Networks, 38, 393–422.
2. Mohanty, P., Panigrahi, S., Sarma, N., &SankarSatapathy, S. (2010). Security issues in wireless sensor network data gathering protocols: A survey. Journal of Theoretical and Applied Information Tech-nology, 13(1), 14.
3. Rassam, M. A., Maarof, M. A., &Zainal, A. (2012). A survey of intrusion detection schemes in wireless sensor networks. American Journal of Applied Sciences, 9(10), 1636–1652.
4. Padmavathi, G., &Shanmugapriya, D. (2009). A survey of attacks, security mechanisms and challenges in wireless sensor networks. International Journal of Computer Science and Information Secu-rity,4(1–2), 1–9.
5. Wang, Y., Attebury, G., & Ramamurthy, B. (2006). A survey of security issues in wireless sensor networks. IEEE Communications Surveys & Tutorials, 8, 2–23.
6. Teodoroa, P. G., Verdejo, J. D., Fernandez, G. M., & Vazquez, E. (2009). Anomaly-based network intrusion detection: techniques, systems and challenges. Computers & Security, 28, 18–28.
7. Alrajeh, N. A., Khan, S., & Shams, B. (2013). Intrusion detection systems in wireless sensor networks: A review. International Journal of Distributed Sensor Networks, 2013, Article ID 167575.
8. Zahariadas, T., Trakadas, P., Maniatis, S., &Karkazis, P. (2009). Efficient detection of routing attacks in wireless sensor networks. In 16th International conference, systems, signals and image processing,
   pp. 1–4, 2009.
9. de Silva, A. P. R., Martins, M. H. T., Rocha, B. P. S., Loureiro, A. A. F., Ruiz, L. B., & Wong, H. C. (2005). Decentralized intrusion detection in wireless sensor networks. Montreal, QC, pp. 16–23.
10. Hu, Y., Perring, A., & Johnson, D. B. (2003) Packet leashes: A defense against wormhole attacks in wireless networks. In Proceedings of 22nd annual conference on IEEE computer and communication society, pp. 1976–1980.
11. Laos, L., Poovendran, R., Meadows, C., Syverson, P., & Chang, W. (2005). Preventing wormhole attacks on wireless ad hoc networks: A graph theoretic approach. IEEE Conference Wireless Com-munications and Networking, 2, 1193–1199.