ISSN 2350-1022

International Journal of Recent Research in Mathematics Computer Science and Information Technology
Vol. 3, Issue 2, pp: (60-66), Month: October 2016 – March 2017, Available at: www.paperpublications.org

An Effective Mechanism to Detect Selective Forwarding Attack in Wireless Sensor Network

S.K.Shaju[1], R.Isaac Sajan[2], Bibin Christopher[3], Dr.A.J.Deepa[4]

[1]PG Scholar, [2,3] Research Scholar, [4]Professor, CSE, Ponjesly College of Engineering, Nagercoil, India

Abstract: **As a promising data gathering and event monitoring technique wireless sensor network (WSN) has been widely applied to both military and civilian applications. Due to the unreliable wireless passage in WSNs, the packet loss gauge during the conveyance of sensor vertex may be highly variant of time. One of the major critical threads is selective forwarding attack, where compromised nodes can maliciously drop a subset of forwarding packet to deteriorate the data delivery ratio of the network. In this paper a modified channel-aware reputation system with adaptive detection threshold to detect selective forwarding attacks in WSNs. The CRS-A evaluates the data forwarding behaviors of sensor nodes, according to the deviation of the monitored packet loss and the estimated normal loss. Extensive simulation results demonstrate that modified CRS-A can accurately detect selective forwarding attacks and identify the compromised sensor nodes, while the attack-tolerant data forwarding scheme can significantly improve the data delivery ratio of the network**.

Keywords: **Wireless Sensor Network, Selective Forwarding attack, Reputation System, Packet Dropping, Channel-aware, Routing.**

I. INTRODUCTION

In recent days, wireless sensor network has become an interesting area of research. Where the nodes are free to move anywhere in network. Due to the non-flexibility of wired network the demand of wireless network has increased. When compare to wired network the wireless sensor networks suffers from lot of security problems, due to the open medium, changing of topology structure and distributed architecture. The wireless sensor nodes are communicates through nonlinear channel. Most popular applications of wireless sensor network are weather monitoring (example: temperature sensor), area monitoring, waste water monitoring, industrial monitoring and military application etc.

This work, we focus specially on Denial of Service (DoS) attack known as selective forwarding attack and it is otherwise called as gray hole attack. Some of the security measures are not suitable for wireless sensor network reason due to resource wastage of both energy and memory. The wireless sensor nodes uses air as a medium to communicate with the neighbor nodes. As it has the limited transmission range, a sensor nodes transferred the information from source to sink through multi-hop transmission. In the multi-hop transmission the information are first transfer to the nearby neighbor and then the process goes on. Mostly the sensor nodes are placed in unfriendly environment. It is difficult to detect some internal nodes that may react as malicious nodes. Such kind of attack related to it is selective forwarding attack. In the selective forwarding attack the nodes will selectively drops some set of packets during the communication period. The black hole attack is something related to gray hole. In black hole attack the node drop all the packets during the communication period. So that the selective forwarding attack has given a special consideration to detect the malicious nodes. The wireless sensor nodes does has the ability to withstand the failure during the communication, due to the noise in communication medium which result in a great loss of data packets.

In certain cases, the sensor nodes get deep sleep or get in to sleep mode in order to save the power and during that period of time the node cannot send and receive the data. So system has to know the reason for the drop of packet, is due to selectively loss the packet or may be any other reason. But in this paper importance has given to the selective forwarding attack. Where some period of time the malicious nodes may be behaves like black hole attack. And the neighboring nodes will get confused and decide to seek distinct routing path for the transmission. An alternative approach is non-cryptographic detection techniques which provide a reliable mechanism. The non-cryptographic technique is used for detecting gray hole attack or selective forwarding attack by analyzing and monitoring the wireless sensor nodes. Similarly in watch dog technique, neighbor node can monitor whether it has forwarded the packet to correct destination or not. By studying more about the selective forwarding attack, it mainly focus on the error-free wireless channel and dropping of packet due to malicious nodes.

The selective forwarding attack is mostly focus on the network layer. This will leads a great loss of data packets in wireless sensor networks. The wireless sensor nodes consists of battery as important component for power source. And the solar panels is used as secondary power supply to the nodes. The energy conservation in a wireless sensor network should be minimized which increases the life-time and can able to provide reliable wireless communication. Next important component in wireless sensor network is storage device. It has only the limited storage capacity. Each node has to collect the information about the neighbor node and uses information to carry out routing very efficient.

Synchronization time is also important parameter in wireless sensor network reason as the lack of accuracy in time may significantly reduce the network lifetime.

II. RELATED WORK

Selective forwarding attack is an important problem to be solved in real world. Reason behind that it has lot of drawback such as degradation of the network performance and loss of packet during the communication. The existing work has been studied. It was categories into two types, acknowledgement based and neighbor surveillance based techniques for data transfer from source to destination.

A) Acknowledgement – based defense techniques:

In this techniques, an acknowledgement is used for safe data transfer from source to destination. For example: Consider there are three nodes named as A, B and C. If the data is transfer from node A to node B after success transfer of data to the destination node B will retransfer the acknowledge to the source. This process will increase the overhead of information in the wireless sensor network. In order to overcome these drawbacks an Enhanced Adaptive ACKnowledgement (EAACK) scheme is used. The EAACK scheme will reduce the overhead of information in wireless sensor network by enhancing the acknowledgement. Normally each node will transfer the acknowledgement to the source node, it is also known as hop to hop acknowledgement where it has high load. Therefore in order to reduce the load in wireless sensor network an enhancing acknowledgement scheme is used where it work as for every two node the single acknowledgement is transmitted. As a result it will reduce the load in wireless sensor network.

B) Neighbor – surveillance based defense techniques:

In this techniques, a special hardware called watchdog and data aggregation is used. For example: Consider a room with size of 10 * 10 where a sensor nodes are randomly placed and the watchdog hardware require data for every 5 minutes from the neighbor node. If the watchdog does not received any data for past 5 minutes from its neighbor node means it will consider the neighbor node as malicious node. Next, one is data aggregation where it will aggregate the whole information from all the neighbor node and fix the malicious node. For example: Consider three temperature sensor node and named the node as A, B and C where placed in same room as nearby location. But the node A, B and C transmit the information of temperature in the room as 50 degree, 49.8 degree and 13 degree respectively. Now by combining all the information or aggregation all the information. We can conclude the node C as malicious node.

But overall this process not so accurate in the detection of malicious nodes in wireless sensor network. However we have develop new technique in order to overcome these drawback.

III. SYSTEM MODEL AND DESIGN GOALS

A. Network Model:

Consider a Wireless Sensor Network, where the nodes are placed in randomly and distributed manner. And the node is denoted by N. On the other hand the sink node or destination node are monitored in regular period of time in an open areas. And the information are transmitted to the sink through Multi-hop routing among the sensor nodes. Sensor nodes are communicate with the neighbor nodes based on IEEE 802.11 DCF. Since the environment is using unstable radio signal therefore it increases the packet loss rate exponential over time. Sensor nodes are deployed in open area like war field, forest area etc. Due to the placement of sensor nodes in open area it causes lack of physical protection and therefore they can compromise the nodes in very easy manner. By the study of existing works, the sensor nodes will monitor the data traffic for the neighbor nodes with the help of watchdog or acknowledgement based techniques. But it is difficult to monitor or distinguish the normal packet loss of data and the packet loss occur due to the malicious nodes.

B. Attack model:

In these model, each node assign a value called as reliability value. Where if the reliability value is low means the probability of getting attack is high and the reliability value is high means the probability of getting attack is low. Here cryptographic technique can be implemented for providing data confidentiality and authentication. For example: Consider the two neighboring sensor nodes A and B. where the data traffic between nodes A and B are partially analyzed. And the node A has assign that node B as normal node and the information will transmit all the neighboring nodes but the real fact behind this the node B is a malicious node. Therefore it is very difficult to judge the malicious node and the proposed technique will detect the malicious nodes in very accurate way.

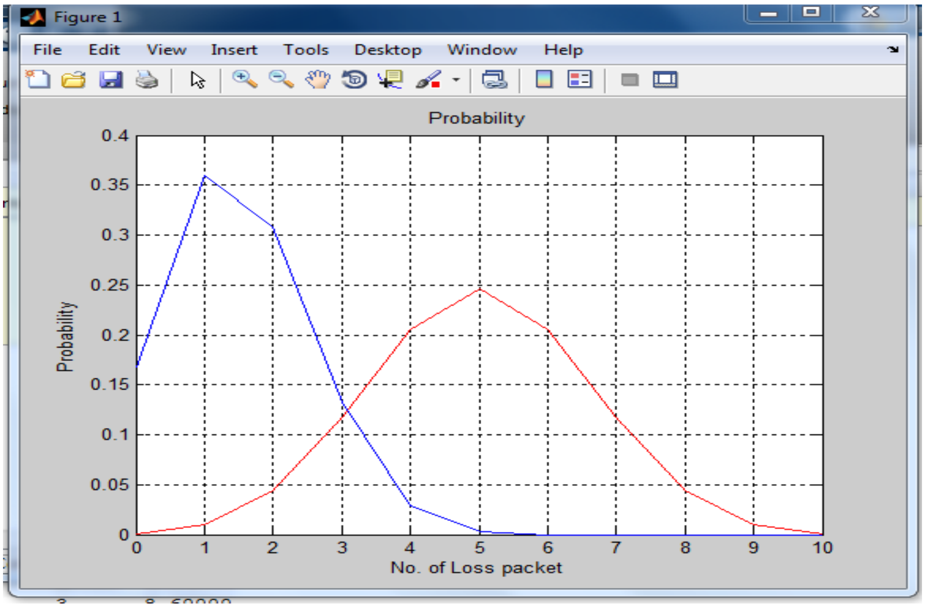

Fig. 1.0 Packet loss occur due to both attack node and without attack node.

C. Design Goals:

The selective forwarding attack is used to monitoring the forwarding traffic information and increase the data delivery ratio. The proposed techniques is focused on the following two goals.

1)Accuracy Detection: The selective forwarding attack has high accuracy in detection of malicious nodes. It has includes the two metric. First, the detection of malicious nodes should have high accuracy. Next, the normal node can be mistakenly identified as malicious node, which creates lot of problem in wireless sensor network.

2) Delivery Rate Increased: Behind the proposed techniques, the data delivery rate has increased by the selective forwarding attack but the negative impact is caused by the attack nodes. Therefore the proposed techniques concentrates on high accuracy in detection of malicious nodes.

IV. THE CLUSTER BASED CHANNEL – AWARE REPUTATION SYSTEM WITH ADAPTIVE DETECTION THRESHOLD.

In the CRS-A section, it includes the following sub task as listed below.

A. Normal Packet Loss Estimation:

In the Wireless Sensor Network, the normal packet loss will occur easily due to the impact of unstable radio environment. Normal packet loss are occur due to the following two aspects as follows.

1) Unstable Radio Link Cause Packet Loss: Due to the poor quality in the radio signal cause the time-varied packet losses. The packet loss rate estimated over a long period of time and the average value shows the time-varied during the evaluation of forwarding behavior.

2) Collision in MAC Layer Cause Packet Loss: The data transmission between two neighbor nodes based on IEEE 802.11 DCF and the MAC layer collision may increase the normal packet loss rate. Since the location of the sensor nodes are static in its location and has fixed number of neighbor nodes.

B. Cluster Head Selection:

In a Wireless Sensor Network for simplifying the complexity of the operation, cluster are used. The cluster is the collection of limited number of devices or nodes. In a cluster the important aspect is selection of cluster header. The cluster header will have the overall responsibility where it will maintain a table called reputation table. The reputation table includes the reputation value where it help to detect the malicious nodes. The selection of cluster head is an elected node which is very nearer to the base station. And the full control goes to the cluster head which is responsible for transmission of data from source to destination.

C. Reputation Evaluation:

The reputation evaluation has includes reputation value where the value is initially fixed as 2. The evaluation of reputation score is performed with the help of first-hand reputation score.

$$\mathrm{r}_{\mathrm{i,j}}{}^{1}(\mathrm{t}) = \begin{cases} +\delta,\ \ if\ m_{i,j}(t) \leq p_{i,j}(t).S_{ij}(t) \\ -\delta, if\ p_{i,j}(t).S_{i,j}(t) < m_{i,j}(t) \leq \varepsilon_{i,j}\ (t) \\ -ƛ, if\ \ m_{i,j}(\mathrm{t})\ >\ \varepsilon_{i,j}(\mathrm{t}) \end{cases} \qquad (1.1)$$

Where, ƛ is a punishment factor and δ is a adjustment factor, we set ƛ≫ δ and the function as follows.

- If $\mathrm{m}_{\mathrm{i,j}}(\mathrm{t}) \leq \mathrm{p}_{\mathrm{i,j}}(\mathrm{t}).\mathrm{s}_{\mathrm{i,j}}(\mathrm{t})$, the sampling test is acceptable.
- If $\mathrm{p}_{\mathrm{i,j}}(\mathrm{t}).\mathrm{s}_{\mathrm{i,j}}(\mathrm{t}) < \mathrm{m}_{\mathrm{i,j}}(\mathrm{t})$, the sampling test is normal.
- When $\mathrm{m}_{\mathrm{i,j}}(\mathrm{t}) > \varepsilon\mathrm{i,j}\ (\mathrm{t})$, the sampling test is misbehave

In the reputation table, entry has been done through the reputation evaluation as the Equation (1.1) has shown above. If the node get loss the packet during the communication the reputation score has been get decreased. Based on above condition and if the packet get transfer successfully means the reputation score get increased. Normally the reputation value is range from 0 to 255.

D. Reputation Propagation:

While forwarding the data from source to destination, it has to improve the attack detection accuracy. Score of reputation is calculated from the neighboring nodes which are called as Second-hand reputation scores. And the equation has shown below.

$$r_{ij}^{2}(t) = \sum_{x \in NCi,g} \frac{Ri,x}{\sum_{s \in NCi} Ri,s}\,.\,r_{x,j}^{1}(t) + \sum_{x \in NCi,b} \frac{Ri,x}{\sum_{s \in NCi} Ri,s}.\,\alpha r_{x,,j}^{1}\ (t) \qquad (1.,2)$$

The Equation (1.2) has shown above is used to repeat the process of calculating reputation score for each and every nodes in the wireless sensor network.

Where α is a penalty factor to reduce the reputation score of the sensor nodes

E. Reputation Integration:;

After the completion of reputation integration and reputation propagation, the first hand and second hand short term reputation score will be integrated together and assign as single entry and update the reputation table in regular period of time.

The below Fig 1.1 shows that the reputation score maintained by each and every nodes in the wireless sensor network.

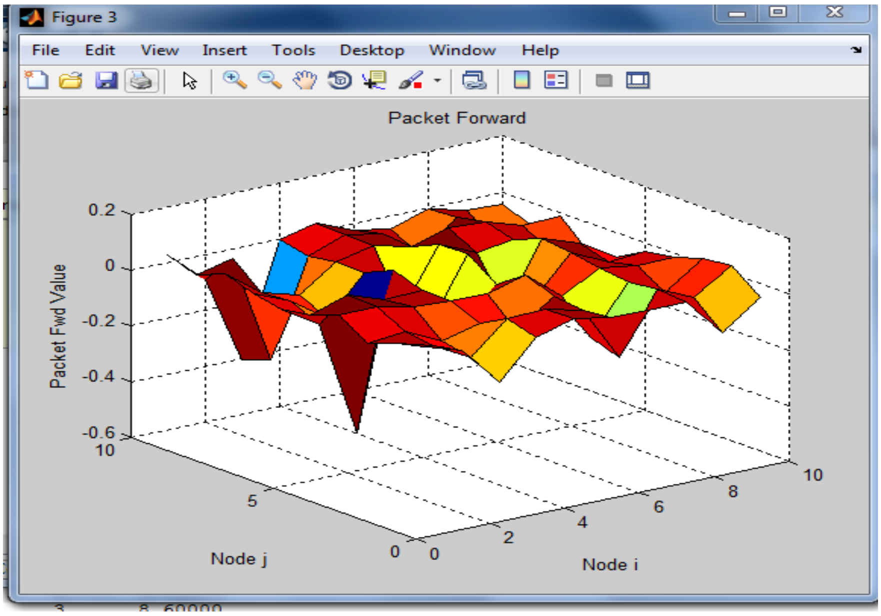

Fig 1.1 Packet Forwarding

The Fig 1.1 shows the packet forwarding between the node i and j based on that the reputation scores is calculated.

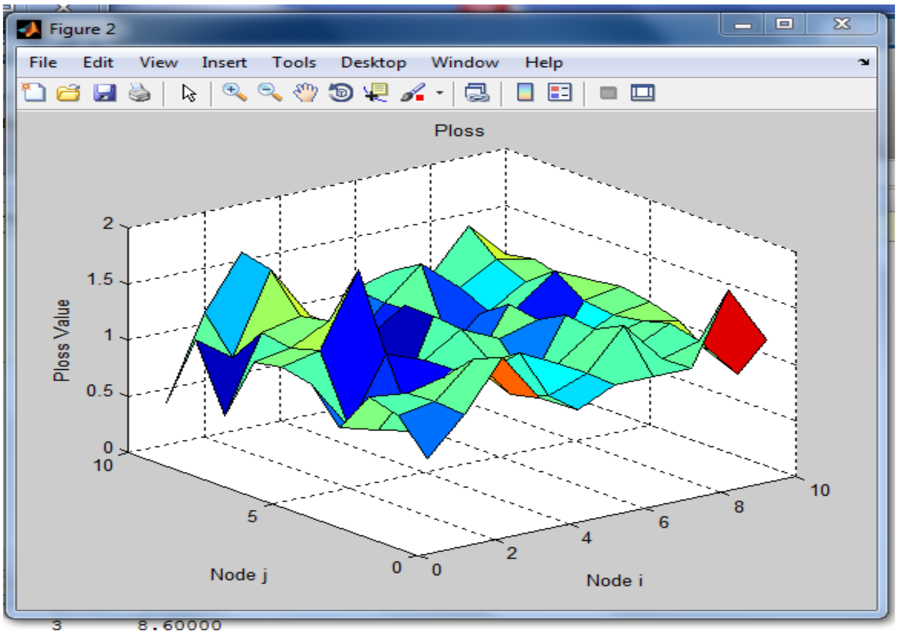

Fig 1.2 Packet Loss

The Fig .1.2 shows the packet loss between the node i and j. It will help to calculate the reputation score for each sensor nodes.

F. Malicious Nodes Identification:

Finally, the identification of malicious nodes is performed with help of reputation table. The reputation value get decrease from 2 if there is packet loss during the transmission of data from source to destination. And the detection of malicious nodes can be performed based on the attack probability value. The attack probability is assign based on the threshold value. The threshold value is calculated based on iterative algorithm. If the reputation value is greater than the attack probability then it is assign as malicious node.

For example: Consider three sensor nodes S, A and B. Where the ten packets are transmitted from S to both A and B. But the node A has loss only one packet during the transmission. And the node B has loss nearly five packet during the transmission. Therefore the normal loss rate is calculated for the node both A and B. The normal loss rate for the node A is 10% and for the node B is 50%. Based on the historical records the attack probability is fixed as 20%. Therefore node B is assigned as malicious nodes due to the dissatisfaction of attack probability value.

V. SIMULATION RESULT

The performance of CRS-A (Channel Reputation System with Adaptive Threshold Detection) with modification and attack tolerant routing scheme are simulated on MATLAB. The simulation consists of 200 stationary sensor nodes uniformly distributed in a 500 x 500m area. The sink node is located at the center of the area. Each sensor node has the probability value in order to compare with the attack probability and find the malicious nodes. The attack probability of each malicious nodes is randomly initialized. Each sensor node generates the data packet of size 10. And the sensor nodes has the transmission range of 85m. Initial the reputation value is 2 for all the sensor nodes. In case of increase of packet loss by the nodes during the communication will also reduce the reputation value from 2.

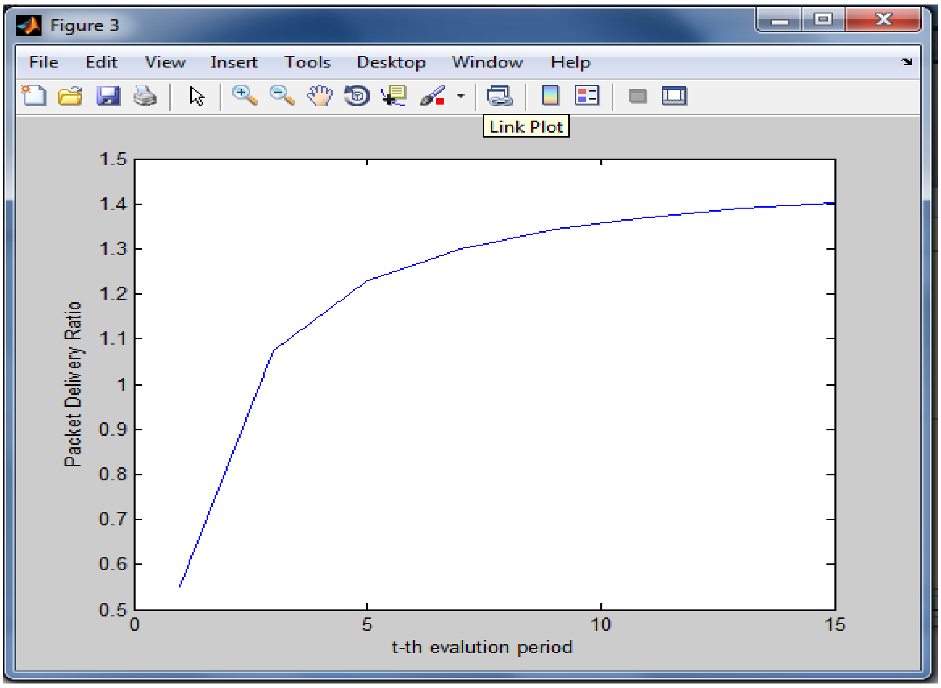

Fig 1.3 Performance Evaluation

The above Fig 1.3 shows that performance evaluation of CRS-A techniques. As a result implementing these technique the detection rate of malicious nodes get increased therefore it will reduce the packet loss rate and improve the performance of the wireless sensor network during communication between the nodes

VI. CONCLUSION

In this paper, a cluster based channel-aware reputation system with adaptive detection threshold (CRS-A) with modification is used to detect the selective forwarding attack in Wireless Sensor Network. Where the proposed system includes high throughput, high rate in detection of malicious nodes

REFERENCES

[1] Baker.M, Giuli.T.J, Lai.K and Marti.S. (2000) ‘Mitigating routing misbehavior in mobile ad hoc networks’, in Proc. ACM MobiCom, pp. 255-256.

[2] Chen.Z, Liu.A, Shen.X, Zhang.C and Zheng.Z. (2012) ‘Secure and energy-efficient disjoint multipath routing for wsns’, IEEE Trans. Vehic. Tech, vol. 61, no. 7, pp. 3255-3265.

[3] Gao.C, Yu.B and Xiao.B. (2007) ‘Chemas: Identify suspect nodes in selective forwarding attacks’, J.Parallel Distributed Comput., vol. 67, no.11, pp. 1218-1230.

[4] Kozma.W, Lazos.L and Zhang.Y. (2013) ‘Amd: Audit-based misbehavior detection in wireless ad hoc networks’, IEEE Trans. Mob. Comput., prePrints. Published online in Sept.

[5] Krunz.M, Lin.S and Shu.T. (2010) ‘Secure data collection in wireless sensor networks using randomized dispersive routes’, IEEE Trans. Mob. Comput, vol. 9, no. 7, pp. 941-954.

[6] Krunz.M and Shu.T. (2012) ‘Detection of malicious packet dropping in wireless ad hoc networks based on privacy-preserving public auditing’, in Proc. ACM WiSec, pp.87-98.

[7] Liang.X, Lin.X and Shen.X. (2014) ‘Enabling trustworthy service evaluation in service-oriented mobile social networks’, IEEE Trans. Parallel Distr. Sys., vol.25, no.2, pp.310-320.

[8] Ren.J Shen.X, Zhang.K and Zhang.Y. (2014) ‘Exploiting channel-aware reputation system against selective forwarding attacks in wsns’, in Proc. IEEE GLOBECOM, pp. 330-335.

[9] Ren.J, Shen.X, Zhang.K and Zhang.Y. (2015) ‘Exploiting mobile crowd-sourcing for pervasive cloud services: challenges and solutions’, IEEE Commun, Mag., vol. 53, no. 3, pp. 98-105.

[10] Shen.W, Wang.X, and Zou.Y. (2013) ‘Physical-layer security with multiuser scheduling in cognitive radio networks’, IEEE Trans. Commun., vol. 61, no 12, pp. 5103-5113.