World Wide Journal of Multidisciplinary Research and Development

WWJMRD 2017; 3(7): 78-81
www.wwjmrd.com
Impact Factor MJIF: 4.25
e-ISSN: 2454-6615

Gurwinder Kaur
Student, Giani Zail Singh College of Engineering and Technology, Bathinda, Punjab, India

Dinesh Kumar
Professor, Giani Zail Singh College of Engineering and Technology, Bathinda, Punjab, India

Correspondence:
Gurwinder Kaur
Student, Giani Zail Singh College of Engineering and Technology, Bathinda, Punjab, India

Imposter detection for replication attacks in mobile sensor networks and reallocating the IDS

Gurwinder Kaur, Dinesh Kumar

Abstract
A wireless sensor network is the wireless network where large number of wireless nodes communicates to each other. These nodes either are moving or can be stationary. While moving and remain stationary they communicate to the environment. Collects the data like temperature, humidity, or soil humidity contents etc. Collected data will be sent to the base station. Which further processes the data?
While setting the network and while communicating in the network various malicious nodes exists. These nodes can copy the characteristics of other legitimate node, this type of node is called as imposter node. Any routed packet from source towards the node with same id will get dropped by the imposter node. Such that packet loss will be taken place. This in results deteriorate the performance of the network.
While identifying the imposter and removing the imposter node from the network, so that node performance should not be hampered. In both the situation the performance has been checked on the basis of various parameters like packet delivery rate, success rate, end to end delay etc. these various performance parameters has shown the improvement. Such that more packet has been transferred and there is more success rate for packets to reach the destination. These factors have been improved due to detection and removal of imposter nodes.

Keywords: Imposter, IDS.

Introduction
Wireless sensor networks are most important technology used in various fields of the daily life. Various sensor nodes positioned in the area Connected wirelessly. These sensor nodes sense the data from the field and send to the base station. If base station is far apart then data sent will be through the relay nodes. In Wireless network various relay nodes are physically positioned. WSN is a network in which nodes are deployed at physical area of interest or very close to that area for monitoring that particular area. The locations of sensors need not to be pre-planned. The position of the sensor node is not pre planned. Sensor nodes are positioned randomly first. Then later on them will be localized w.r.t each other. These wireless sensor nodes are connected to each other wirelessly. They will send the data from one sensor node to the other sensor node. Also while sending the data they will process the data.

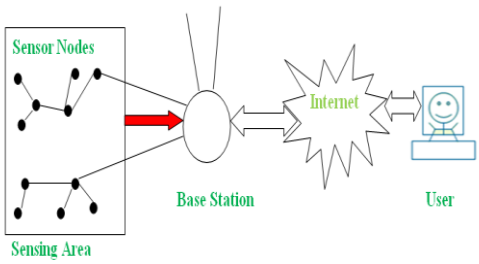


Fig.1.1: A general layout of a wireless sensor network [1]

What is Imposter?
In a MWSN, however, the constant movement of nodes makes location-based detection a nearly impossible task. As a result, an adversary can assume the identity of a legitimate node and use it to communicate with the rest of the network. As sensor nodes are not tamper-

resistant devices [1], the adversary can create *replicas* of nodes after compromising a node and replicating its cryptographic or other material. We refer to such replicas as *imposters* if they use the identity of existing sensor nodes to communicate with the sink or other nodes of the network.

How Replication attacks is detected and removed

Mobile sensor network where nodes relay information among themselves and, if necessary, sensed data can reach base station through the use of appropriate MWSN routing algorithms. To detect an imposter the following simple mechanism is used: "When two sensor nodes meet for the first time, each node generates a random nonce, stores it in its memory, and sends it to the other node. The next time these nodes meet again, they request each other for the values they exchanged in their previous meeting. If a node cannot reply or replies with the wrong number then it is treated as an imposter and the ID of the node is considered compromised." Hence the nonce values are used to detect existence of imposters and they are changed after each successful communication and maintained in a nonceList. The nonceList is maintained individually by each node and contains the nonce values expected from other nodes as well as the values to be sent to other nodes for successful authentication. To exemplify this authentication process further in which two nodes u and v meet for the first time at time t1, exchange their nonces and then each one follows its random path. At some earlier time, an adversary was able to compromise node v and create an imposter with the same ID. Node u, unaware of this event, meets again with a node bearing the ID of v at time t2, thus it expects to receive the nonce it sent to v during the previous encounter at time t1. The imposter i_v is unable to provide this information, thus u knows that ID of v has been compromised.

Literature Survey

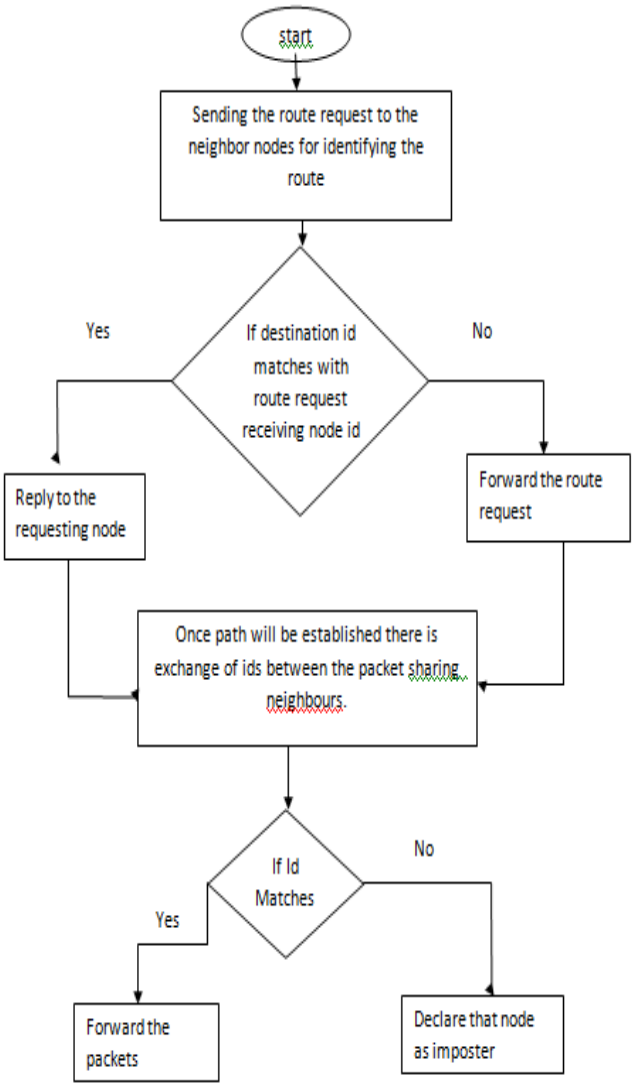
1. Tassos Dimitriou(2016) et al: In this research paper they have come up with replication attack. Where any node relicates the identity of other node. While removing the replication node legitimate node is also removed from the network.
2. Li Lei(2016) et al: this paper has put up the research in malicious node identification in wsn. So that the performance of the nwtrok should not be downgraded.
3. paramveer singh(2015) et al: In this paper they have studied different types of attacks. who they make network highly vulnerable to performance down gradation.
4. Ramnik Singh(2017) et al: Acording to this paper wsn each node senses the physical or environmental parameters by employing the low cost sensor devices. various protocols are suitable for different types of situations.
5. Kemi Ding(2016) et al: This paper has taken up the study to tackle the denial of service attacks. the sensor needs to choose a single channel for sending data packets while reducing the probability of being attacked.
6. Anouar Abdelhakim Boudhir(2013) et al: Localization is the most prevalent issue as far as WSN technology is concerned. It includes various nodes positioned themselves so that whole area will be covered.

Algorithm

There are multiple sequence of steps are being taken through which the work of identifying and removal of imposter node will be removed.

1. Bind the wireless sensor network with various sensor nodes moves from one position to the other position.
2. Broadcast the route request from source node to its immediate neighbours.
3. Each neighbor compare the destination number with its own if it matches the send the route reply. Else will forward the route request.
4. In this way multiple routes will be established at source. One route will be selected having minimum number of intermediate hops.
5. Each node while sending the data packet to the next node in the route table shares the unique id.
6. If the exchanged id matches the previously shared id the packet will be sent. Else the node will be declared imposter. In this way the legitimate node carrying the same number will also be identified as malicious node.
7. Reallocate the new ids to the nodes so that legitimate node which was declared imposter can again be the part of the network.

Flowchart



Network Simulation Setup

SIMULATION PARAMETERS	
COVERAGE AREA	800m x 500m
PROTOCOLS	AODV
NUMBER OF NODES	50
SIMULATION TIME	100 seconds
TRANSMISSION RANGE	250m
MOBILITY MODEL	RANDOM WAY POINT MODEL
LOAD	5 Kb-UDP Packets
MOBILITY SPEED(variable)	20 Seconds
TRAFFIC TYPE	CBR
PACKET SIZE	512 Kbps
PAUSE TIME	10

Table 1.1: network configuration

Results

Mobility of Nodes

The Creation of Clusters with 20 mobile nodes as it shown in the NAM console which is a built in program in NS-2-allinone package after the end of the simulation process. Here the scenario of Mobility of nodes consists of

- Packet Forwarding
- Packet Dropping
- Movement of Nodes

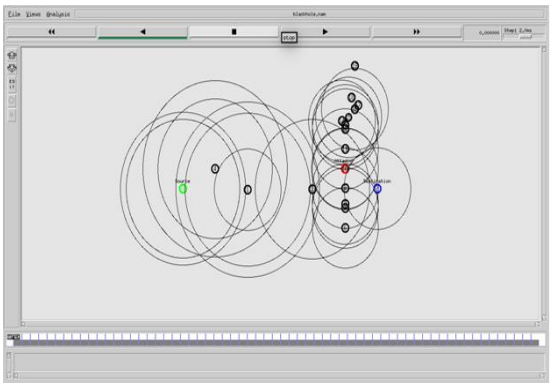


Fig. 1.2: Creation of Cluster with 50 nodes

Comparison

Packet Delivery Ratio

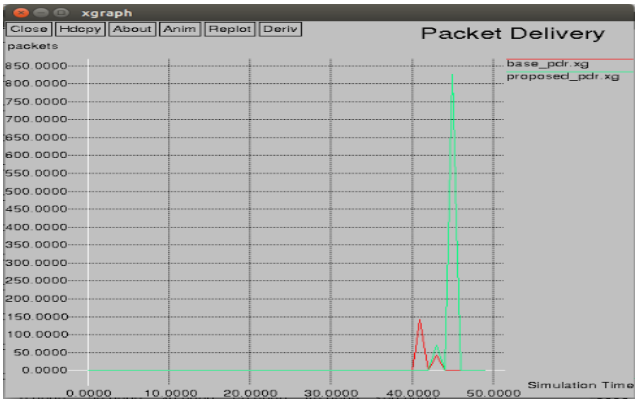


Fig. 1.3: Packet Delivery ratio

Packet delivery in case of current research and base paper has been compared. In current research the packet are delivered more compared to the base paper. In previous research as reallocation of ids does not be taken place. So till that time node remain out of the communication. That means the count of legitimate node will be reduced. But in current research the reallocation of ids are being taken place. So that legitimate nodes again become part of the communication.

Success Rate

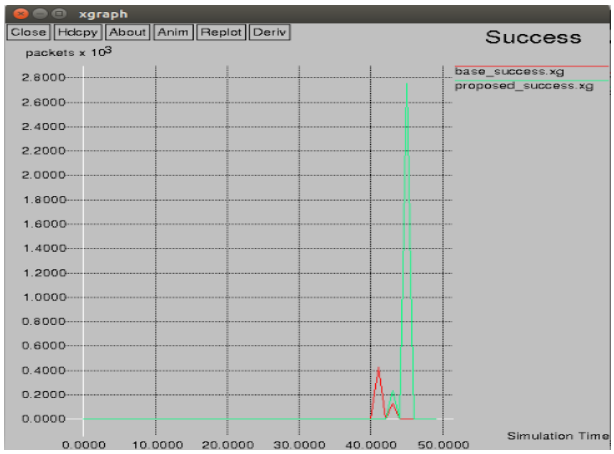


Fig. 1.4: Success rate graph.

There is an improvement in the success rate for current research. More packets will be delivered success fully in case of current research compared to the base technique. Because no legitimate node will remains out of the network. It is done in current research by reallocating the ids to the nodes.

End to End Delay

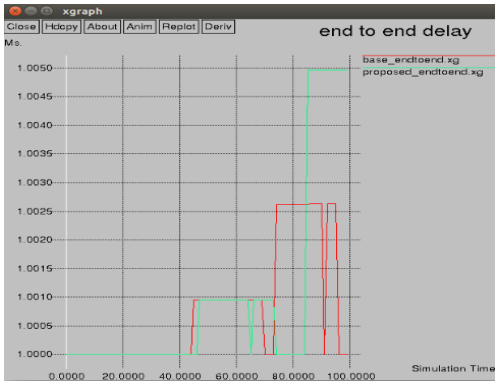


Fig. 1.5: End to End Delay

In end to end delay comparison for both current research and previous research is taken place. End to end delay for current research is little more. Because at intermediate there is reallocation of ids. That will take some time. In result will slow up the whole process. But by little more end to end delay more packet delivery is successfully get.

Conclusion

In wsn sensor nodes collects the data from its location and send that data to the base station. At intermediate level there can be imposter type node, which copies the identity of the legitimate node. Every time while sending and receiving the data there is exchange of the ids. If the nodes exchanged ids matches the previously communicated ids then node is declared legitimate node else will be declared

imposter node. Also reallocation of ids are being taken place. Once the procedure is completed there is enhancement of the performance. There is more success rate and more packet delivery ratio. But there is more end to end delay. On the basis of these performance it can be seen that with little increase of the end to end delay there is more packet delivery ratio.

Future Work

In future more study has to be taken place for enhancement of the results. In future more work can be taken place to reduce the end to end delay.

References

1. Tassos Dimitriou a, Ebrahim A. Alrashed b, ∗, Mehmet Hakan Karaata b, Ali Hamdan," Imposter detection for replication attack s in mobile sensor networks", Computer Networks 108 (2016) 210–222
2. LiLei_WenYang_ChaoYang,"Event-based distributed state estimation over a WSN with false data Injection Attack, IFAC-PapersOnLine 49-22 (2016) 286–290
3. Karanpreet Singh, Paramvir Singh, Krishan Kumar," A systematic review of IP traceback schemes for denial of service attacks", S0167-4048(15)00093-0
4. Ramnik Singh1, Anil Kumar Verma" Energy Efficient Cross Layer based Adaptive Threshold Routing Protocol for WSN", S1434-8411(16)30621-5
5. M.S. Aruna, Ridha Bouallegue, and E. Cayirci, "Comparative study of learning-based localization algorithms for Wireless Sensor Networks," Computer Networks J., 38(4), 393–422, 2015.
6. Gabriele Oliva, D. Evans, "Localization for Wireless Sensor Networks:protocols and Perspect," Proc. 10th Annual Int. Conf. on Mobile Computing and Networking, Philadelphia, PA, USA, 2015.
7. Xin Tan and S.S. Iyengar, "Localization in Cooperative Wireless Sensor Networks: A Review,"
8. M. R. Ghafouri Fard, "Angle of Arrival Localization for Wireless Sensor Networks," Ravi chander Janapati, H.C. So, W.K. Ma, Y.T. Chan, ''Received Signal Strength Based Mobile Positioning via Constrained Weighted Least Squares,'' Proc. of Int. Conf. on Acoustics, Speech, and Signal Processing (ICASSP 2003), vol. 5, 2015.
9. Kai Yik Tey, H. Lichtenegger, and J. Collins, Global Positioning System: Theory and Practice, 3 rd ed. New York, NY: Springer-Verlag, 2014.
10. Chen Liang, H. Balakrishnan, E. Demine, and S. Teller, "Anchor Free Distributed Localization in Sensor Networks," Tech Report "Designing a positioning system for finding things and people indoors,".
11. Hanen Ahmadi, C. Lanzl, "Designing a positioning system for finding things and people indoors," *Spectrum, IEEE*, 35(9), 71-78, 2013.
12. Yao-Hung Wu, "A distributed location system for the active office," *IEEE Network*, 8(1), 62-70, 2013.