WWJMRD 2017; 3(11): 379-383
www.wwjmrd.com
International Journal
Peer Reviewed Journal
Refereed Journal
Indexed Journal
UGC Approved Journal
Impact Factor MJIF: 4.25
e-ISSN: 2454-6615

Jaspreet Singh
Student, Guru Kashi
University, Talwandi Sabo,
Bathinda, Punjab, India

Rachna Rajput
Professor, Guru Kashi
University, Talwandi Sabo,
Bathinda, Punjab, India

Correspondence:
Jaspreet Singh
Student, Guru Kashi
University, Talwandi Sabo,
Bathinda, Punjab, India

Replication Node Detection in Mobile Sensor Networks Based Routing For Peer To Peer Data Sharing

Jaspreet Singh, Rachna Rajput

Abstract

A wireless detector network is that the wireless network wherever sizable amount of wireless nodes communicates to every alternative. These nodes either are moving or may be stationary. Whereas moving and stay stationary they communicates to the setting. Collects the info like temperature, humidity, or soil humidness contents etc. Collected knowledge are sent to the bottom station. That any processes the info. Whereas setting the network and whereas act within the network numerous malicious nodes exists. These nodes will copy the characteristics of alternative legitimate node, this sort of node is termed as impostor node. Any routed packet from supply towards the node with same id can get born by the impostor node. Specified packet loss are taken place. This in results deteriorate the performance of the network.

While characteristic the impostor and removing the impostor node from the network, so that node performance shouldn't be hampered. In each things the performance has been checked on the premise of varied parameters like packet delivery rate, success rate, finish to finish delay etc. these numerous performance parameters has shown the development. Specified a lot of packet has been transferred and there's a lot of success rate for packets to achieve the destination. These factors are improved thanks to detection and removal of impostor nodes.

Keywords: Imposter, IDS.

Introduction

Wireless device networks (WSNs) square measure most significant technology during this century. WSN composed of assorted nodes referred to as sensors. By the advancement in space of electronics mechanical systems (MEMS) still as wireless communication technology tiny, low cost and good sensors square measure positioned in physical space and connected through wireless links and also the net provides outstanding opportunities for numerous applications. WSN may be a network during which nodes square measure deployed at physical space of interest or terribly near that space for observance that individual space. The locations of sensors needn't to be pre-planned. Embedded microprocessors and radio transceivers square measure combined with sensors nodes. Device nodes square measure used for sensing the info, process the info and for communication purpose. These deployed sensors square measure connected with wireless association. Sensors sense info specific space during which they're deployed and forward that data to the common purpose for additional process on it information.

.

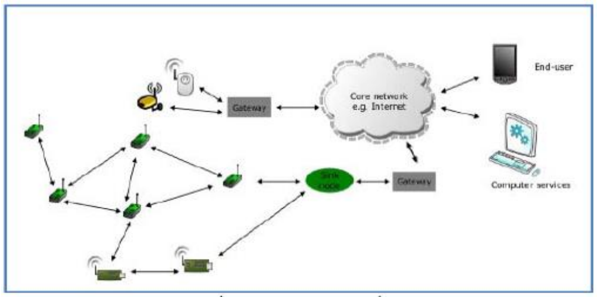


Fig.1.1: A general layout of a wireless sensor network [1]

What is Imposter

Imposter is the node which takes the identity of another node and try to behave in same way as the legitimate node behaves. But this node which is generating the copy of the nodes will not be having no legal id to share. Sometime this node can be indulge in dropping the packets.

How Replication attacks is detected and removed

In mobile ad-hoc network various nodes intercommunicates to each other. While doing that they share the data amongst each other. In MANET there is no central controller which can control the identity of the any node which is becoming the part of the network. At any point of time any node become part of the network as well as taken out of the network. Imposter node is one of the problem of the MANET. To detect this node each node share the previously allocated ids with each other. If the id shared is correct then the node will be declared legitimate. Else the node will be declared imposter node. For any further communication they will be stopped from being part of the communication. This is how the imposter node will be detected.

Literature Survey

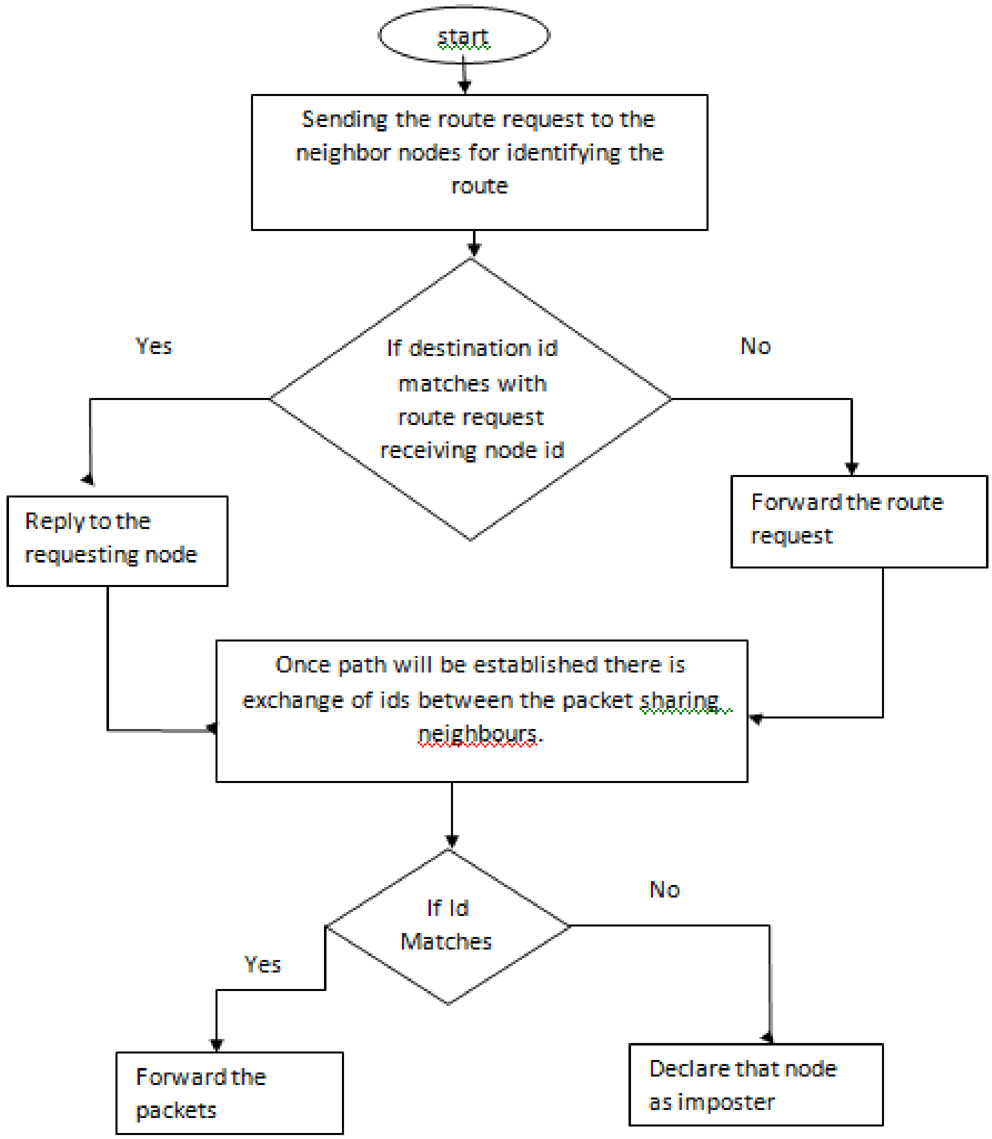
1. Tassos Dimitriou(2016) et. al: this paper has proposed an algorithm based on sharing ids amongst various nodes before sending and receiving the data. Any node which is new to the communication will be allocated with new id. And later on if node is legitimate then only it is allowed to share the data amongst each other.
2. Li Lei (2016) et al: this paper has proposed a technique to share secured contents amongst sensor node and the base station. If the preset conditions are full filled then only they will share the data. Else the node will be stopped from communication.
3. Paramveer singh(2015) et al: this research paper has conducted a survey on various types of denial of service attacks. Such that these wireless networks are highly vulnerable to various types of attacks. These wireless sensor networks are not specifically ment to meet these kinds of attacks.
4. Ramnik Singh (2017) et al: Wireless Sensor networks are the special types of the network. It includes various sensor nodes communicated to the mobile station. These mobile sensor nodes are to collect the data from their physical environment. Collect that data and send that data to the base station.
5. Kemi Ding (2016) et al: This paper considers a cyber-physical system (CPS) under denial-of-service (DoS) attacks. The measurements of a sensor are transmitted to a remote estimator over a multi-channel network, which may be congested by a malicious attacker. Among these multiple communication paths with different characteristics and properties at each time step, the sensor needs to choose a single channel for sending data packets while reducing the probability of being attacked. In the meanwhile, the attacker needs to decide the target channel to jam under an energy budget constraint. To model this interactive decision making process between the two sides, we formulate a two-player zero-sum stochastic game framework.
6. Anouar Abdelhakim Boudhir (2013) et al: Localization has newly received research interest due to the success of the emerging wireless sensor network (WSN) technology. This interest is expected to grow further with the proliferation of wireless sensor network applications such as medicine, military, transport.In this context routing, protocols and technologies of communication on those wireless area are enormously applied to sensor networks in order to improve the quality of service and communication.

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. Collect various sensor nodes for building wireless sensor networks.
2. Send request from the source sensor node to immediate neighbor nodes.
3. Neighbor nodes wither forward the route request or will reply with the destination.
4. At source multiple path will be collected. One path will be selected having shortest route in terms of distance.
5. Send the data packets on to the specified route.
6. Share the exchange ids, to declare node to be legitimate else malicious.
7. Once the legitimate node will be out of communication will be reallocated with new ids.

Flowchart


start
Sending the route request to the neighbor nodes for identifying the route
If destination id matches with route request receiving node id
Yes
No
Reply to the requesting node
Forward the route request
Once path will be established there is exchange of ids between the packet sharing neighbours.
If Id Matches
No
Yes
Forward the packets
Declare that node as imposter

Network Simulation Setup

Table 1.1 Network configuration

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

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

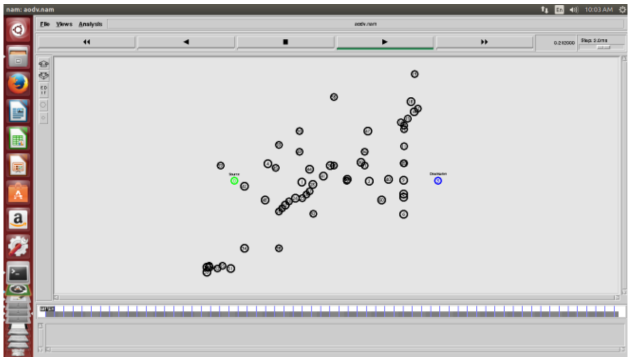


Fig.1.2: Creation of Cluster with 50 nodes

Comparison

Success Rate

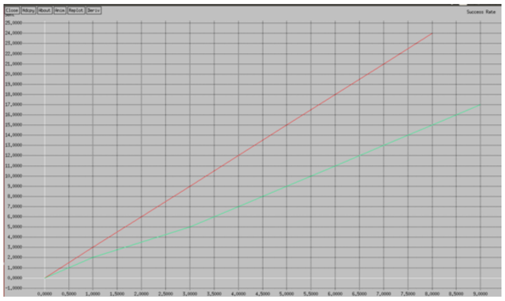


Fig 1.3 Success rate

Success Rate comparison between existing and proposed research has shown that the packet delivery become better in case of proposed research.

Response Time

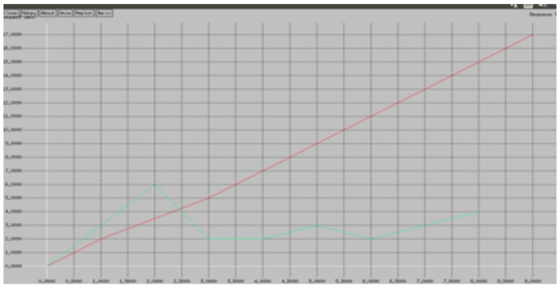


Fig 1.4: Response rate graph

Success rate in case of proposed technique has improved compared to the existing research. Because reallocate the ids will make node to be the part of the communication.

Mac Load

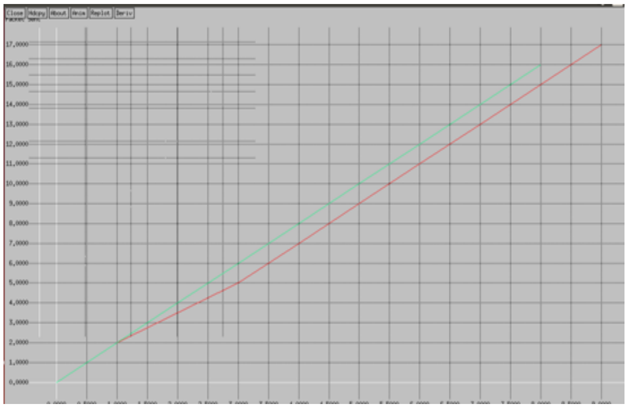


Fig. 1.5 Mac Load Delay

In proposed technique end to end delay has improved. That means less time will be delayed once the reallocation to ids will be done.

Improvement

Parameters	Improvement
Success rate	23%
Response Time	19%
MAC Load	9%
Throughput	18%
Hop To Hop Delay	7%
Packet Dropped	45%
Routing Load	6%

Conclusion

In Wireless sensor network various sensor nodes collect the data from their physical environment. The data collection is always a regular exercise. After the time period the collected data will be transferred to the base station. While transferring the data any malicious node can read the data. To protect the system from such kind of replication attack ids are exchanged. So that only those node will participate in communication who has legitimate ids. All the parameters line success rate, end to end delay and packet delivery ration has shown the improvement.

Future Work

Wireless sensor network is highly vulnerable to various kinds of attacks. To mitigate the attacks id exchange is taken place. This exchange has increase the end to end delay. In further research end to end delay can be improved.

References

1. Xin Tan and S.S. Iyengar, "Localization in Cooperative Wireless Sensor Networks: A Review,"
2. 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.
3. Kai Yik Tey, H. Lichtenegger, and J. Collins, Global Positioning System: Theory and Practice, 3 rd ed. New York, NY: Springer-Verlag, 2014.
4. 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,".
5. Hanen Ahmadi, C. Lanzl, "Designing a positioning system for finding things and people indoors," *Spectrum, IEEE*, 35(9), 71-78, 2013.
6. Yao-Hung Wu, "A distributed location system for the active office," *IEEE Network*, 8(1), 62-70, 2013.
7. Neal Patwari and V. Padmanabhan, "RADAR: An in-building RF-based user location and tracking system" *Proc. Of INFOCOM*, pp. 775–784, March 2013.
8. S. Alireza Motevallian, A. Chakraborthy, and H. Balakrishnan,"The cricket location support system," *Proc. of ACM/IEEEInt. Conf. on Mobile Computing and Networking (MOBICOM)*, August 2013.
9. Mostafa Mofarreh-Bonab, J. Heidemann, and D. Estrin. "GPS-less Low Cost Outdoor Localization for Very Small Devices," *IEEE Personal Communications Magazine*, 7(5), 28-34, Oct. 2013.
10. 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
11. LiLei_WenYang_ChaoYang,"Event-based distributed state estimation over a WSN with false data Injection Attack, IFAC-PapersOnLine 49-22 (2016) 286–290
12. Karanpreet Singh, Paramvir Singh, Krishan Kumar," A systematic review of IP traceback schemes for denial of service attacks", S0167-4048(15)00093-0
13. Ramnik Singh1, Anil Kumar Verma" Energy Efficient Cross Layer based Adaptive Threshold Routing Protocol for WSN", S1434-8411(16)30621-5
14. [13] 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.
15. [14] 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.