IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 1, January 2016

Poly Tree Construction Method to improve QoS in Wireless Sensor Networks

Nirupama. A[1], Sudarson Jena[2]

Research Scholar, Department of CSE, GITAM University, Hyderabad, India[1]

Associate Professor, Department of IT, GITAM University, Hyderabad, India[2]

Abstract: The recent developments in Wireless Sensor Networks (WSN) suffer from efficient and secure transmission of packets. The common attacks in WSN are dropping/modification of data packets. Security to the data can be improved by disconnecting the droppers/modifiers form the network. This paper proposes a method to identify the nodes which are droppers and to disconnect them from the network. Simulation results are presented.

Keywords: WSM, Packet Droppers, Modifiers, Multihop, Misbehaving Nodes.

I. INTRODUCTION

The multi hop communication in the wsn suffer from secured end to end transmission of packets. The top layers in the wsn consists of internet entry point, routers and access points etc. the bottom layer consists of mobile network users. As the Wireless Sensor Network (WSN) consists of spatially distributed self-dependent sensors it is difficult to provide security to the data. Packet dropping and modification are common attacks in multi hop wsn which can be launched by an adversary to disrupt the communication channel. The nodes in the network can be compromised with the malicious users. An intruder may launch various attacks in the network even if a single node gets compromised [1]. Multipath forwarding of packets can be used in which packets are forwarded along multiple redundant paths to ensure that at least one path cannot tolerate packet dropping [2], [3], [4], [5]. The modified packets can be filtered and can be en-routed with a certain number of hops [6], [7], [8], [9]. Nodes can continuously monitor the forwarding behaviour of their neighbours to locate and identify packet droppers and modifiers to determine if the neighbours are misbehaving, which has been proposed in [10], [11], [12], [13], [14], [15]. The reputation based mechanism to identify whether a non-neighbour node is trustable or not is presented in [15], [16], [17].

The sensor nodes are deployed randomly in a two dimensional area. These sensors periodically generate sensory data and collaborate with each other to forward the data towards a sink node, which is located within the network. A bad node can be any node within the network which will drop or modify the data in the packets to degrade the performance of the network. To identify these bad nodes it is required for each node to continuously monitor the forwarding behaviour of its neighbours to determine if they are behaving. The misbehaving of a node can be measured by using reputation mechanism to identify whether a non-neighbour node is trustable or not. The existing work shows that the modified packets are not filtered and the nodes remain same. These modified packets are used as evidence to infer packet modifiers.

This paper proposes a technique to drop the nodes which are identified as bad nodes and the network is restructured to construct a poly tree. The newly constructed poly tree consists of trustable nodes.

II. POLY TREE CONSTRICTION METHOD (PTCM) TO IMPROVE QOS IN WSN

Poly Tree Constriction Method to improve QoS in WSN, to identify the bad nodes which ae misbehaving in the network, the sensor nodes forms a polytree by removing the cycles within the network. Routing path is established from this poly tree. The data is forwarded through this path to the sink. Each packet sender/forwarder adds a small extra bit to each packets and encrypts the packet and forward it towards the sink. After each round the sink nodes runs a node categorization algorithm to identify bad nodes based on the reputation. All the sensor nodes form a poly tree which contains no cycles and routing path is established towards a sink node. The sink node is aware of the poly tree and shares a unique key with each node. When a node wants to transmit a packet to the sink node it adds the key shared with the sink node and forwards it to its parent node towards sink. The intermediate node adds an extra bits and encrypts the packet and forwards it towards sink node. If the intermediate node is a bad node it may drop or modify the packet

Advantages of PTCM:

The data is transmitted through multiple redundant paths to ensure that at least one route delivers the packets successfully to the sink. As the Poly tree does not contain any cycles and consists of trustable nodes the data will be delivered successfully at the sink which increase the quality of the network.

As the bad nodes are deleted and the network is reconstructed after each round, the data has to travel less which increase the throughput of the network. Designed such that the sink can obtain very useful information from the marks. Specifically, based on the packet marks, the sink can figure out the dropping ratio associated with every node.

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 1, January 2016

III. RESULTS & DISCUSSIONS

The objective is to propose a simple method to catch both packet droppers and modifiers. The following performance metrics are used to identify bad nodes in the network

Throughput: amount of received by a sink node from source within a given time.

End to End delay: the average time interval between the generation of packets at source and the successful delivery of the packet at the destination node

Packet Delivery Ratio (PDR): PDF is defined as the ratio between number of packets delivered by source and number of received by the sink node.

```
==============================
Catching Packet Droppers in WSN
==============================
Enter No. of  Nodes: 35
Enter Transmission Range : 150
INITIALIZE THE LIST xListHead
Locating node(0) :(89.828838636087653,202.63276538002901)
Locating node(1) :(61.109677684078775,56.28226904956729)
Locating node(2) :(420.1198950969241,364.06151520277444)
Locating node(3) :(477.35751628752683,358.22099557063586)
Locating node(4) :(275.34069459668393,120.84326917344856)
Locating node(5) :(266.0312476875406,149.74390759586538)
Locating node(6) :(432.31870463691592,384.3750661166269)
Locating node(7) :(239.67027768477345,110.68563838986942)
Locating node(8) :(366.90552316927608,64.90232481849489)
Locating node(9) :(16.716530554330223,363.78322130245306)
```

Fig 1. Simulation results for 35 nodes

In this paper the results are obtained from NS2, the analysis is carried out for the network with the 35 nodes WSN, with a transmission range of 150m. Figure 1 shows the simulation setup for 35 nodes.

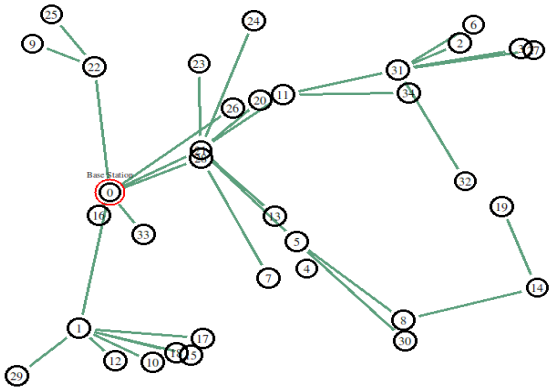

Fig. 2. Tree Routing of nodes

Figure 2 gives the network is generated with tree routing structure for the 35 nodes where node 0 is considered as the base station.

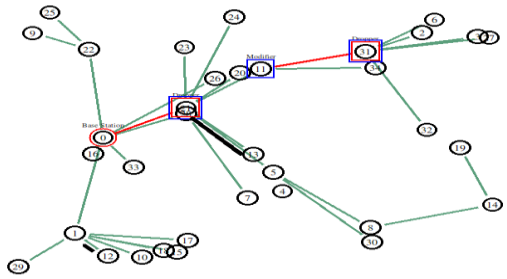

Fig. 3. Packet Droppers and Modifier Detection

Figure 3 shows the packet droppers and modifiers which are identified by calculating the PDR at each node and are considered as bad nodes

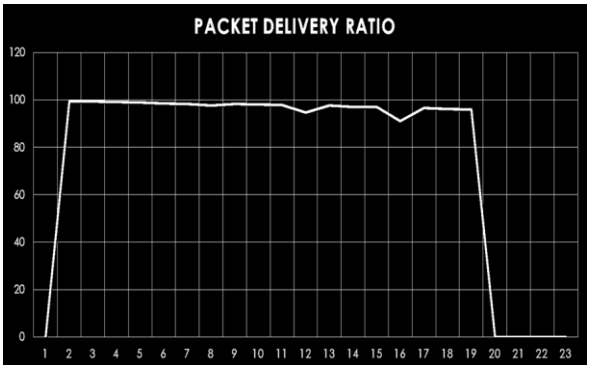

Fig 4. Packet Delivery Ratio

In figure 4 the time interval to PDR is considered as 2 seconds and nodes are considered with an interval of 10. The PDR is increasing with the time interval as the bad nodes are eliminated.

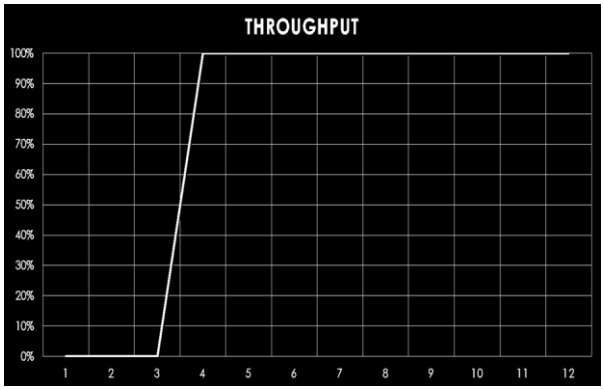

Fig 5. Throughput

The time interval to calculate throughput is considered as for 100 seconds and nodes are considered with an interval of 5 which is shown in figure 5. The throughput remains constant when the bad nodes are eliminated.

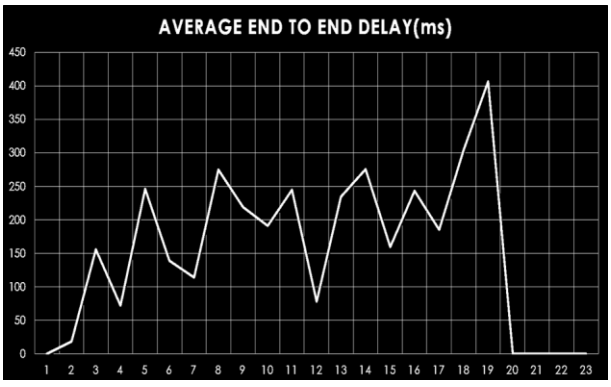

Fig 6. Average End to End Delay

Figure 6 shows time interval to calculate average end to end delay which is calculated for every s 50 seconds and nodes are considered with an interval of 5.

IV. CONCLUSION

This paper proposes a Poly Tree Construction method by deleting cycles in the graph and to provide security as well

DOI 10.17148/IJARCCE.2016.5182

improve the QoS by deleting the misbehaving nodes. A routing path is established at the end of each round after deleting the bad nodes

REFERENCES

[1]. Catching Packet Droppers and Modifiers in Wireless Sensor Networks by Chuang Wang, Taiming Feng, Jinsook Kim, Guiling Wang, Member, IEEE, and Wensheng Zhang,
[2]. H. Chan and A. Perrig, "Security and Privacy in Sensor Networks," Computer, vol. 36, no. 10, pp. 103-105, Oct. 2003.
[3]. V. Bhuse, A. Gupta, and L. Lilien, "DPDSN: Detection of Packet-Dropping Attacks for Wireless Sensor Networks," Proc. Fourth Trusted Internet Workshop, 2005.
[4]. M. Kefayati, H.R. Rabiee, S.G. Miremadi, and A. Khonsari, "Misbehavior Resilient Multi- Path Data Transmission in Mobile Ad-Hoc Networks," Proc. Fourth ACM Workshop Security of Ad Hoc and Sensor Networks (SASN '06), 2006.
[5]. I. Khalil and S. Bagchi, "MISPAR: Mitigating Stealthy Packet Dropping in Locally-Monitored Multi-Hop Wireless Ad Hoc Networks," Proc. Fourth Int'l Conf. Security and Privacy in Comm. Netowrks (SecureComm '08), 2008.
[6]. F. Ye, H. Luo, S. Lu, and L. Zhang, "Statistical En-Route Filtering of Injected False Data in Sensor Networks," Proc. IEEE INFOCOM, 2004.
[7]. S. Zhu, S. Setia, S. Jajodia, and P. Ning, "An Interleaved Hop-by-Hop Authentication Scheme for Filtering False Data in Sensor Networks," Proc. IEEE Symp. Security and Privacy, 2004.
[8]. S.Ganeriwal, L.K. Balzano, and M.B. Srivastava, "Reputation-Based Framework for High Integrity Sensor Networks," ACM Trans. Sensor Networks, vol. 4, no. 3, pp. 1-37, 2008.
[9]. W. Li, A. Joshi, and T. Finin, "Coping with Node Misbehaviors in Ad Hoc Networks: A Multi-Dimensional Trust Management Approach," Proc. 11th Int'l Conf. Mobile Data Management (MDM10), 2010.
[10]. P. Michiardi and R. Molva, "Core: A Collaborative Reputation Mechanism to Enforce Node Cooperation in Mobile Ad Hoc Networks," Proc. IFIP TC6/TC11 Sixth Joint Working Conf. Command Multimedia Security: Advanced Comm. and Multimedia Security, 2002.
[11]. Q. Li and D. Rus, "Global Clock Synchronization in Sensor Networks," Proc. IEEE INFOCOM, 2004.
[12]. K. Sun, P. Ning, C. Wang, A. Liu, and Y. Zhou, "Tinysersync: Secure and Resilient Time Synchronization in Wireless Sensor Networks," Proc. 13th ACM Conf. Computer and Comm. Security (CCS '06), 2006.
[13]. H. Song, S. Zhu, and G. Cao, "Attack-Resilient Time Synchronization for Wireless Sensor Networks," Ad Hoc Networks, vol. 5, no. 1, pp. 112-125, 2007.
[14]. B. Xiao, B. Yu, and C. Gao, "Chemas: Identify Suspect Nodes in elective Forwarding Attacks," J. Parallel and Distributed Computing, vol. 67, no. 11, pp. 1218-1230, 2007.
[15]. S. Buchegger and J. Le Boudec, "Performance Analysis of theConfidant Protocol," Proc. ACM MobiHoc, 2002.
[16]. S. Ganeriwal, L.K. Balzano, and M.B. Srivastava, "Reputation-Based Framework for High Integrity Sensor Networks," ACMTrans. Sensor Networks, vol. 4, no. 3, pp. 1-37, 2008.
[17] W. Li, A. Joshi, and T. Finin, "Coping with Node Misbehaviors in Ad Hoc Networks: A Multi-Dimensional Trust Management Approach," Proc. 11th Int'l Conf. Mobile Data Management (MDM'10), 2010.

DOI 10.17148/IJARCCE.2016.5182