International Journal of Computer Network and Security(IJCNS)
Vol 8. No.1 –2016 Pp. 17-20

available at : www.ijcns.com
ISSN: 0976-1345

Reduction of False Positives using Optimal Node Selection in MANET

Jayashree S Patil[1] , Dr.K.V.N.Sunitha[2]
[1]G. Narayanamma Institute of Technology and Science (for Women) Shaikpet,
[1]Hyderabad - 500104, Telangana State, India.
[2]BVRIT Hyderabad College of Engineering for Women, Hyderabad, Telangana
[1]jshivshetty@gmail.com,[2]k.v.n.sunitha@gmail.com

Abstract

Mobile Ad-hoc Network (MANET) is a self configuring network which allows nodes to enter the network and also leave the network in a random manner without notification to the network. This dynamic nature allows the malicious nodes to enter the network and attack other legitimate node. To ensure the security in network it is necessary to detect attacks or malicious nodes and notify the network. In this paper, we have proposed an algorithm for Reducing False Positives using Optimal Node selection in MANET. This technique raises an alarm if any node detects its neighbour to be malicious and then it is validated to check for false alarm. In this way, network performance is enhanced by utilizing the optimal nodes with lesser security costs for further traffic handling.

Keywords: Malicious Node, Optimal Node, False Positives, Security Cost

1. Introduction

1.1 Mobile Ad-hoc Network (MANET)

MANET is basically made up of several mobile nodes which can also perform the functions of a router. MANET is used widely used due to factors like node mobility, wireless network type, effective linking ability with other nodes. In applications where the user is not fixed and keeps moving continuously, then this network type becomes very useful. In MANET, several nodes enter into the network and some also get removed out of the network. This may occur due to several causes [1].

A Mobile Adhoc Network is a collection of independent mobile nodes that can communicate to each other via radio waves. The mobile nodes that are in radio range of each other can directly communicate, whereas others need the aid of intermediate nodes to route their packets. Each of the nodes has a wireless interface to communicate with each other. These networks are fully distributed [2].

1.2 Characteristics of MANET

MANET has many features which is critical to its network performance. Some of the important characteristics of MANET are:
1. Dynamic topology
2. Distributed Network Operation
3. Light weight and autonomous terminals
4. Shared physical medium

1.3 Limitations in MANET

MANET faces several disadvantages due to its features like infrastructure less network type, dynamic topology, etc. Some of the major limitations faced by MANET are:
1. Lack of central node to control the network operations.
2. Node operations should be performed with care so as to avoid the issue of running out of the power supply.
3. No precise boundary line: Since nodes can enter and exit the network in a random manner, it is not possible to consider any specific boundary.
4. Scalability: The dynamic nature mobile nodes make it a difficult task to maintain the scalability of the network.
5. Security concerns: In MANET, the malicious nodes to attack the network and cause security issues.
6. Resource Unavailability: No specific resource allocation process in MANET because of the distributed architecture. [3].

1.4 Advantages of MANET

There are few advantages of MANET because of its dynamic nature these are:
1. The nodes also function as routers in MANET.
2. Design cost is reduced because MANETS are infrastructure less.
3. Distributed nature of the network reduces the operation cost.
4. Its self healing as nodes keeps moving dynamically [4].

1.5 False Alarms in MANET

False alarms may occur when the nodes in network plays as selfish. A false alarm protocol, also called alert alarm, is erroneous report of presence of malicious node in network, causing unnecessary changes where they are not needed. Efficient and timely False alarm protocol becomes a prime task of intrusion management of mobile ad hoc network, a prerequisite for good utilization of packets on the network, and a crucial feature for the usability of mobile ad hoc networks [5].

There are two types of false alarm protocol. They are:
1. False alarm protocol for Infrastructure network.
2. False alarm protocol Infrastructure less network.

2. Related Works

Guo Yuanbo et al [8] have proposed a mechanism Design Based Nodes Selection Model for Threshold Key Management in MANETs. In this paper we formulated the dynamic nodes selection problem as a combinatorial optimization problem firstly, with the objectives of maximizing the success ratio of key management service and minimizing the nodes' cost of security and energy, and then proposed the incentive compatible mechanism to implement the optimal nodes selection process in MANETs, to ensure the truth-telling is the dominant strategy and so prevent the emergence of selfish nodes.

Shiau-Huey Wang et al [9] have proposed An Exchange Framework for Intrusion Alarm Reduction in Mobile Ad-hoc Networks. Our model selects the node with the best connectivity as the temporary centralized node for collecting all local alarms. Subsequently, it utilizes majority-voting strategy to detect false alarms. After false alarm reduction, an accurate local alarm is broadcast as a global alarm for notifying the entire network of the attacker existence. This model has the advantages of alarm reduction and low time overhead. The experimental results demonstrate that our solution is scalable and is not influenced by mobility. Extra alarm exchange and verification messages cause low time and message overhead.

Jianfeng Ma et al [10] have proposed Incentive-Based Optimal Nodes Selection

Mechanism for Threshold Key Management in MANETs with Selfish Nodes. Then, to ensure truth telling is the dominant strategy for any node in our scenario, we extend the payment structure of the classical Vickrey-Clarke-Groves (VCG) mechanism design framework and divide the payment into pieces to the nodes, with the consideration of their actual execution effectiveness. Simulations show that the proposed mechanism enjoys improvements of both the success ratio of key management service and lifetime of the network, as well as reductions of both the cost of participating nodes and compromising probability of MANETs, compared with the existing work.

3. Proposed algorithm for Reducing False Positives using optimal node selection in MANET

3.1 Overview

In this work, we propose to design **algorithm for Reducing False Positives using optimal node selection.**In this mechanism, after estimating the trust values from the monitoring nodes, the co-ordinator node.In order to reduce the false positives and the information overhead, the alarm exchange and reduction mechanism [9] is applied. In this mechanism, the alarms or intrusion detection warnings from the monitoring nodes will be aggregated by the co-ordinator and validated. Then a global alarm will be broadcast by the co-ordinator. Thus, the proposed solution performs reduction of false-positives using the optimal node.

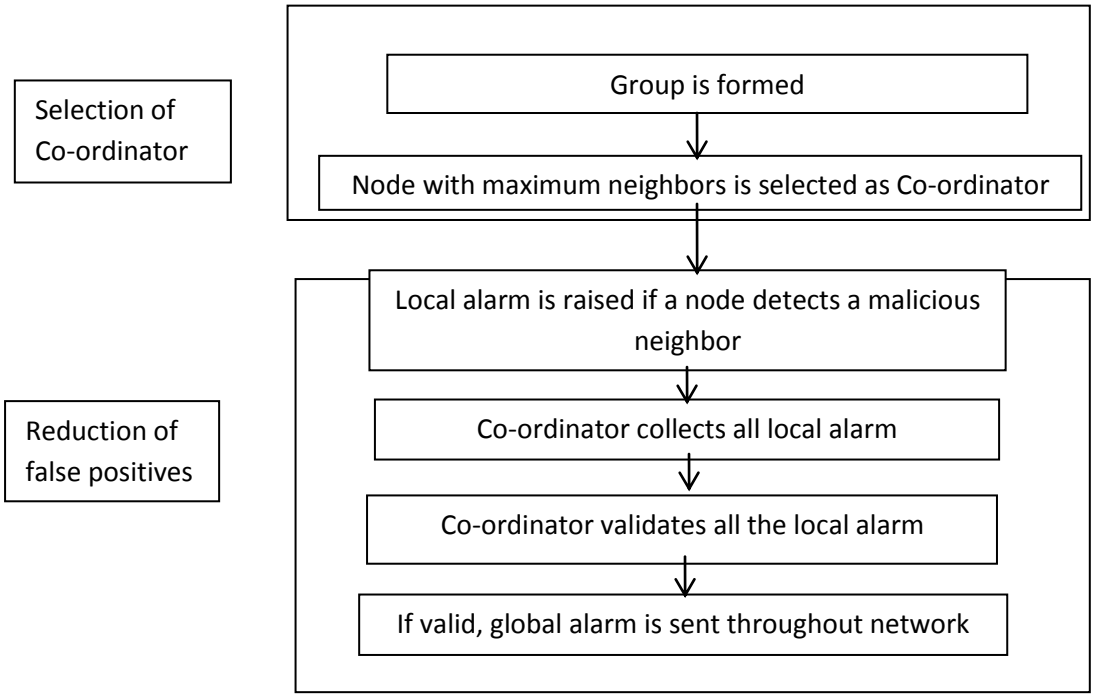


Fig. 1: Block Diagram

3.2 Selection of Co-ordinator Node

In this technique, MANET is divided into several smaller groups based on the hop distances. In each group, a co-ordinator is selected [9]. It is responsible for handling the network operations effectively. The process of co-ordinator selection is described in algorithm 1.

Algorithm 1

1. Each node in the network monitors its one-hop neighbour node and each node in turn is

also monitored by its surrounding one-hop neighbour nodes.
2. All nodes within two hop distance form a G.
3. Each member of a G, maintains information about the one hop neighbours of all its one hop neighbour nodes.
4. The node with maximum number of one hop neighbours is selected as a C.
5. If more than one node in the G, has maximum number of one hop neighbours, then the nodes with lowest MAC address is selected as a C.

After the selection of the Co-ordinator in every group in the network, then it performs the group based operations to enhance the overall network operations.

3.3 Reduction of False Positives

Intrusion Detection in the network is critical to ensure network security. During intrusion detection in the network, nodes which detect any malicious nodes, raise local alarm to notify the co-ordinator node [9]. Then the co-ordinator node validates each alarm in order to avoid any false alarm. This process is described in algorithm 2.

Algorithm 2

1. The member nodes send a A_{Local} to its C whenever it suspects any of its neighbour to be malicious.
2. C collects A_{Local} from all its members.
3. If the link between any member and C is broken, then the C will wait for the A_{Local} for a T_{th} .
4. If the C does not receive the A_{Local} from the disconnected member within the T_{th}, then C sends a AREQ to that member.
5. On receiving AREQ, the member resends the A_{Local}.
6. Then based on the received A_{Local}, the C initiates the validation process.
7. To validate each A_{Local} case, raised w.r.t a suspicious neighbor by other members, the C considers N_{raised} and N_{not_raised}.
8. If $N_{raised} > N_{not\_raised}$, then the A_{Local} is considered as valid alarm.
9. $N_{raised} < N_{not\_raised}$, then the A_{Local} is considered as false alarm.
10. All the false alarms are ignored by the C.
11. The valid A_{Local} is then converted into a A_{Global} and is broadcasted throughout the network through the nodes with minimum costs detected in algorithm 2.

Thus, the false alarms are detected and avoided. This helps in avoiding the extra costs incurred due to security compromise.

4. Simulation:

4.1 Simulation Parameters

We use NS2 to simulate our proposed **Reducing False Positives using optimal node selection.** (RFPON) protocol. We use the IEEE 802.11 for wireless sensor networks as the MAC layer protocol. It has the functionality to notify the network layer about link breakage. In our simulation, the number of nodes is varied as 20,40,60,80 and 100. The area size is 1000 meter x 1000 meter square region for 50 seconds simulation time. The simulated traffic is Constant Bit Rate (CBR).

4.2 Performance Metrics

We evaluate performance of the new protocol mainly according to the following parameters. We compare the (EFIAR) [9] protocol with our proposed RFPON protocol.

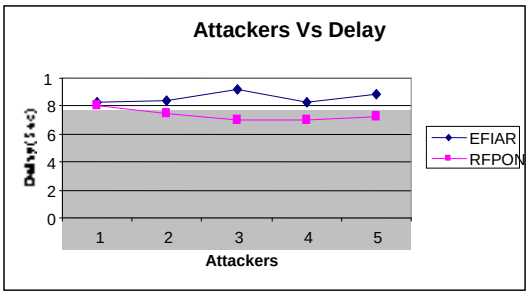
Average Packet Delivery Ratio: It is the ratio of the number of packets received successfully and the total number of packets transmitted.
Residual Energy: It is the amount of energy remains in the nodes after the data transmission.
Throughput: The throughput is the amount of data that can be sent from the sources to the destination.
Packet Drop: It is the number of packets dropped during the data transmission

4.3 Results & Analysis

The simulation results are presented in the next section.

Based on Attackers

In our experiment we vary the number of attackers as 1,2,3,4 and 5.



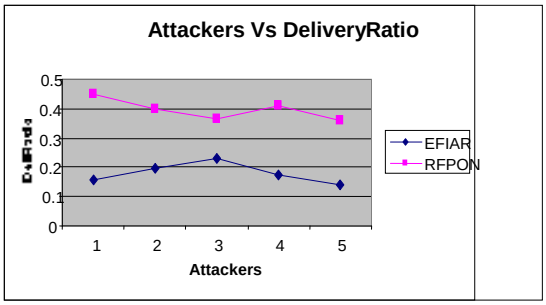
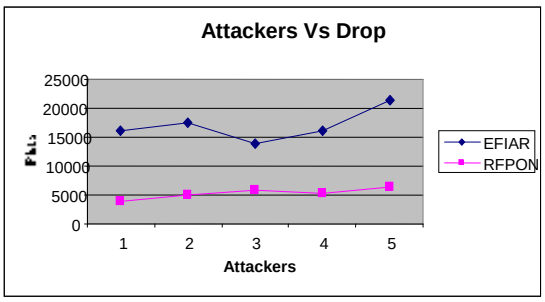


Fig 2: Attackers Vs Delay

Fig 3: Attackers Vs Delivery Ratio



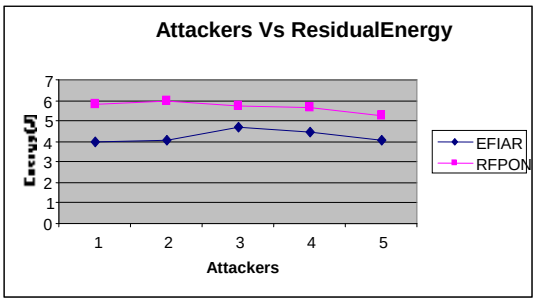


Fig 4: Attackers Vs Drop

Fig 5: Attackers Vs Residual Energy

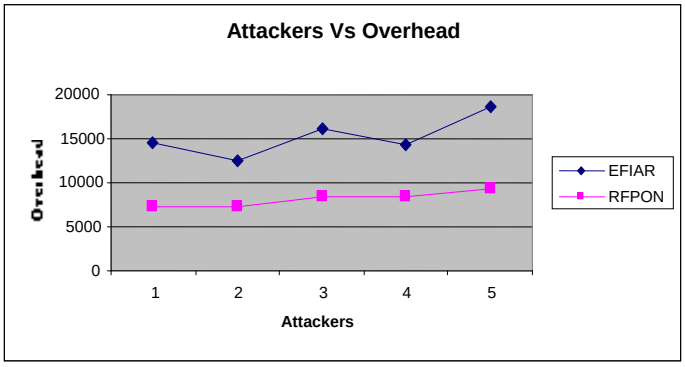


Fig 6: Attackers Vs Overhead

Figures 2 to 6 show the results of delay, delivery ratio, packet drop, residual energy and overhead by varying the number of attackers from 1 to 5 for the CBR traffic in RFPON and EFIAR protocols. When comparing the performance of the two protocols, we infer that RFPON outperforms EFIAR by 14% in terms of delay, 54% in terms of delivery ratio, 69% in terms of drop, 25% in terms of residual energy and 47% in terms of overhead.

5. Conclusion

In this paper, we have proposed Reducing False Positives using optimal node selection in MANET. Initially, the entire network is divided into smaller groups. In each group, a co-ordinator node is selected to handle all the group members. Then within each group, nodes with minimum security costs are selected. When a member node suspects its neighbor to be malicious, it sends a local alarm to its co-ordinator. Co-ordinator node collects all the local alarm sent by its group members and validates it. If the alarm is detected to be valid, then the co-ordinator node generates a global alarm and broadcasts it throughout the network. Thus, ensuring that the node selection process is optimal the false alarms raised in the network are also kept minimal.

References:

1. P. Suma, O. Nagaraju and Md. Ali Hussain, "Cost Optimal Random Path Selection Algorithm for Security in MANETS", www.ijird.com, International Journal of Innovative Research and Development, ISSN 2278 – 0211 (Online), January, 2016, Vol 5 Issue 2.

2. Aarti and Dr. S. S. Tyagi, "Study of MANET: Characteristics, Challenges, Application and Security Attacks", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 5, May 2013, ISSN: 2277 128X.

3. Priyanka Goyal, Vinti Parmar and Rahul Rishi, "MANET: Vulnerabilities, Challenges, Attacks, Application", IJCEM International Journal of Computational Engineering & Management, Vol. 11, January 2011, ISSN (Online): 2230-7893, www.IJCEM.org

4. D. Helen and D. Arivazhagan, "Applications, Advantages and Challenges of Ad Hoc Networks", Journal of Academia and Industrial Research (JAIR), Volume 2, Issue 8 January 2014

5. Dr. S. Parryselvam and K. Yazhini, "A Survey of False Alarm Protocol for Mobile Ad-hoc Networks", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 6, Issue 3, March 2016, ISSN: 2277 128X

6. Ms. I.Shanthi and Mrs. D. Sorna Shanthi, "Detection of false alarm in handling of selfish nodes in MANET with congestion control", IJCSI International Journal of Computer Science Issues, Vol. 10, Issue 1, No 3, January 2013, ISSN (Print): 1694-0784 | ISSN (Online): 1694-0814, www.IJCSI.org

7. M. Sandhini and S. Saravanan, "False Alarm Method for Detecting Selfish Node in Manet", International Journal of Future Generation Communication and Networking", Vol. 9, No. 5 (2016), pp. 43-48, http://dx.doi.org/10.14257/ijfgcn.2016.9.5.05.

8. GUO Yuanbo, MAJianfeng, WANG Chao and YANG Kuiwu, "Mechanism Design Based Nodes Selection Model for Threshold Key Management in MANETs", Chinese Journalof Electronics, Vol.22, No.4, Oct. 2013

9. Shiau-Huey Wang, "An Exchange Framework for Intrusion Alarm Reduction in Mobile Ad-hoc Networks", JOURNAL OF COMPUTERS, VOL. 8, NO. 7, JULY 2013

10. Yuanbo Guo, Jianfeng Ma, Chao Wang, and Kuiwu Yang, "Incentive-Based Optimal Nodes Selection Mechanism for Threshold Key Management in MANETs with Selfish Nodes", Hindawi Publishing Corporation, International Journal of Distributed Sensor Networks, Volume 2013, Article ID 416983,13pages, http://dx.doi.org/10.1155/2013/416983