International Journal of Engineering Studies.
ISSN 0975-6469 Volume 8, Number 2 (2016), pp. 199-210

https://dx.doi.org/10.37622/IJES/8.2.2016.199-210

Optimal Node Selection and Alarm Exchange Technique for Reducing the Security Cost and False Positives in MANET

Jayashree S Patil[1] and Dr. K.V.N. Sunitha[2]

[1]G Narayanamma Institute of Technology and Sciences, India.

[2] BVRIT Hyderabad College of Engineering for Women, India.

Abstract

Mobile Ad-hoc Network (MANET) is a wireless network consisting of numerous nodes which are move every minute and are highly mobile. Basically, MANET is a self configuring network where nodes can enter the network and also leave the network in a random manner without prior notification to the network. This allows the malicious nodes to enter the network and attack other legitimate node. Hence, to ensure security in the network it is necessary to detect attacks or malicious nodes and notify the network. In this paper, we have proposed an Optimal Node Selection and Alarm Exchange Technique for Reducing the Security Cost and False Positives 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 nodes with lesser security costs for further traffic handling.

Keywords: Optimal Node, Alarm exchange, Security Cost, False Positives

1. INTRODUCTION

1.1 Mobile Ad-hoc Network (MANET)

A MANET is a type of network with mobile nodes. Each node in this mobile adhoc network works as a router. The moving capability of nodes, wireless facility, and best connectivity with other moving nodes of the network makes MANETs very attractive. These facilities made the need for MANETS increase enormously. The areas where moving nodes are desirable wish to use this type of network. When all the nodes in a network are in motion, many nodes are added and many gets discarded from the network for various reasons [1].In MANET, there are numerous member nodes and each node link with the other nodes through radio waves. During network communication, the nodes which are within the transmission range of each other, communicate directly. But when the nodes are not within the transmission range, then the intermediate nodes forward and route the packets towards the destination. In MANET, every node communicates wirelessly and in a distributed manner [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. Distributed Network Operation
2. Multihop Routing
3. Autonomous Terminal
4. Shared physical medium
5. Dynamic topology
6. Light weight terminals [2]

1.3 Limitations in MANET

1. MANET faces several disadvantages due to its features like infrastructureless network type, dynamic topology, etc. Some of the major limitations faced by MANET are:
2. Absence of central managing entity: Since MANET is a distributed network, its network operation is distributive in nature and hence there is no centralized node to control the network operations.
3. Limited Power Supply: The highly mobile nodes in MANET are provided with lesser power storage ability. Also, during mobility and traffic handling process, large amount of power gets consumed. So, node operations should be performed with care so as to avoid the issue of running out of the power supply.

4. Absence of precise boundary line: Since MANET is a self configuring network where nodes can enter and exit the network in a random manner, it is not possible to consider any specific boundary. This makes the entry of malicious nodes very easy and makes the network prone to attacks.
5. Scalability: The dynamic nature of the newtork due to the highly mobile nodes makes it a difficult task to maintain the scalability of the network.
6. Security issues: In MANET, since the nodes can enter the network without fulfilling any specific criteria, it becomes easy for the malicious nodes to attack the network and cause security issues.
7. Resource Inavailability: Since MANET is a distributed network, there is no specific resource allocation process. Hence sometimes, the availability of resources for every nodes can not be assured [3].

1.4 Advantages of MANET

Due to the distributed nature and dynamic topology of the MANET, it enjoys many advantages. Some of the advantages of MANET are:

1. The nodes in MANET, also function as routers.
2. Since MANET is wireless, there is no need of any infrastructure and hence design cost is lesser.
3. Operation costs are comparatively lesser due to the distributed nature of the network.
4. The frequent reconfiguration in the network, allows self healing [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].
In MANET, false alarms is seen when network node becomes a selfish node and transmits false message stating some other node in the network to be malicious. A false alarm protocol is also referred as alert alarm and is basically an inaccurate report indicating a member node to be compromised. In MANET, checking for false alarm in a regular manner is necessary to ensure efficent network performance [5].
There are two types of false alarm protocol. They are:

1. Infrastructured network based false alarm protocol.
2. Infrastructureless network based false alarm protocol.

2. RELATED WORKS

Ms. I. Shanthi et al [6] have proposed a technique for Detection of false alarm in handling of selfish nodes in MANET with congestion control. In this paper, the false alarm is detected and this detected information is given to all the nodes along the transmission path regarding the location where the link is broken, so that the another better transmission route can be chosen to transfer the traffic. This does not allow any degradation in network performance even during congestion. This technique basically detects the attacking node and then informs the remaining members of the network.

Guo Yuanbo et al [8] have proposed a mechanism Design Based Nodes Selection Model for Threshold Key Management in MANETs. The issue of dynamic node selection is handled as a integrative optimization issue. Initially, the success ration of the key management service is increased and then the security cost and energy cost incurred at every node is reduced.

Shiau-Huey Wang et al [9] have proposed An Exchange Framework for Intrusion Alarm Reduction in Mobile Ad-hoc Networks. In this technique, initially a node with good connectivity is selected as centralized node and it gathers all the local alarms sent by the remaining nodes, by this false alarm is reduced. Next, the basic local alarm is modified into a global alarm and broadcasted to the entire network. This notifies all the network members of the existence of the malicious node in the network. This technique minimizes false alarm and lowers the time overhead, it is scalable and not affected by mobility. However, message overhead can occur in the network if there are extra alarm exchange and verification messages.

3. PROPOSED OPTIMAL NODE SELECTION AND ALARM EXCHANGE TECHNIQUE FOR REDUCING THE SECURITY COST AND FALSE POSITIVES IN MANET

3.1 Overview

In this work, we propose to design an optimal node selection and alarm exchange mechanism that concentrates on reducing the false positives and overall cost of the detection system.In this mechanism, after estimating the trust values from the monitoring nodes, the co-ordinator node determines the total cost of each node. The cost can be estimated from the security state S^t_i and energy state E^t_i [10] of the i_{th} node at stage t. It then chooses the nodes which minimizes the total cost value.

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 security cost and false-positives.

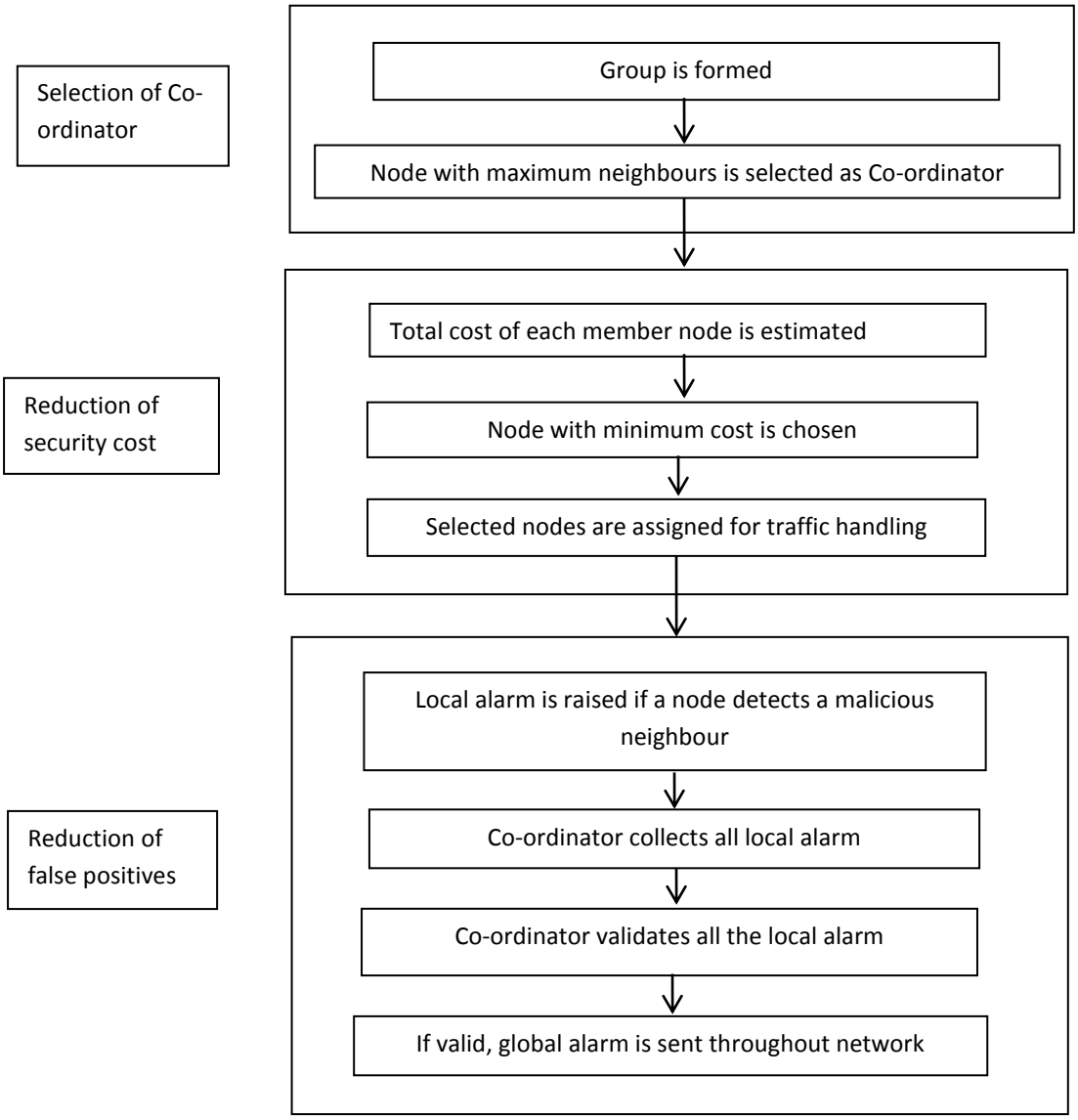

Fig. 1: Block Diagram

3.2 Selection of Co-ordinator Node

In this technique, the 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
Notations:

1. G : Group
2. C : Co-ordinator

Algorithm:

1. Each node in the network monitors its one-hop neighbor node and each node in turn is also monitored by its surrounding one-hop neighbor nodes.
2. All nodes within two hop distances form a G.
3. Each member of a G, maintains information about the one hop neighbors of all its one hop neighbor nodes.
4. The node with maximum number of one hop neighbors is selected as a C.
5. If more than one node in the G, has maximum number of one hop neighbors, 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 Security Cost

During network operations, the maintenance of network security is given high priority. Hence the security cost in network is usually high. The security cost in the network can be reduced by using nodes with lesser security maintenance needs [10]. Selection of nodes with lesser costs is described in algorithm 2.

Algorithm 2

Notations:

1. i : integer number of node
2. t : stage of node
3. S^t_i : security state of node i at stage t
4. E^t_i : energy state of node i at stage t
5. A^t_i : action adopted by node i at stage t
6. $c(S^t_i, A^t_i)$: security cost
7. $c(E^t_i, A^t_i)$: energy cost
8. TT^t_i : total cost of node i at stage t
9. α. : weight factor of two costs

Algorithm:

1. The $c(S^t_i, A^t_i)$ for S^t_i is considered.
2. The $c(E^t_i, A^t_i)$ for E^t_i is considered.
3. The TT^t_i total cost of node i at stage t is dependent on the S^t_i and E^t_i as described by equation (1).

$$TT^t_i (S^t_i, E^t_i, A^t_i) = (1-\alpha).\ c(S^t_i, A^t_i) + \alpha.\ c(E^t_i, A^t_i) \quad (1)$$

4. The TT^t_i is calculated in accordance with the network lifetime as shown in equation (2).

$$TT^t_i (S^t_i, E^t_i, A^t_i) = [(1-\alpha).\ c(S^t_i, A^t_i) + \alpha.\ c(E^t_i, A^t_i)]/A^t_i \quad (2)$$

5. In this way, the TT^t_i for all nodes in the network is estimated.

1. The nodes with minimum TT^t_i are selected.
Nodes with lesser cost consume lesser energy and provide more secure communication between the nodes in the network. Only the nodes with minimum total costs are selected for the transmission of important information such as carrying local alarms, etc.

3.4 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 inorder to avoid any false alarm. This process is described in algorithm 3.

Algorithm 3
Notations:

1. A_{Local} : Local Alarm
2. C : Co-ordinator
3. T_{th} : predefined time interval to receive local alarm
4. AREQ : Alarm Request
5. N_{raised} : number of neighbors raising local alarm
6. N_{not_raised} : number of neighbors who didn't raise local alarm
7. A_{Global} : Global Alarm

1. The member nodes send a A_{Local} to its C whenever it suspects any of its neighbor 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 dectected 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 Optimal Node Selection and Alarm Exchange Technique for Reducing the Security Cost and False Positives (ONSAET) 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 ONSAET 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

A. Based on Nodes: In our simulation we vary the number of nodes as 20,40,60,80 and 100.

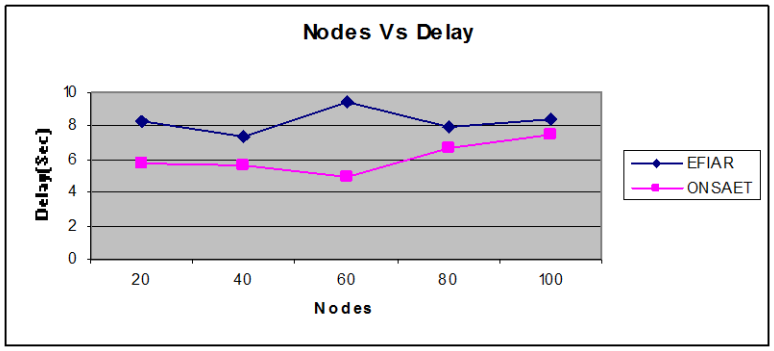

Fig 2: Nodes Vs Delay

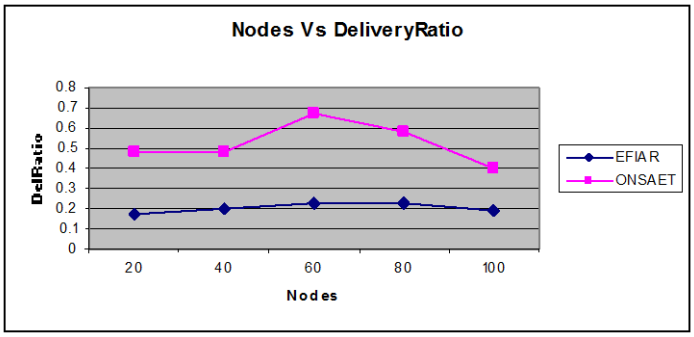

Fig 3: Nodes Vs Delivery Ratio

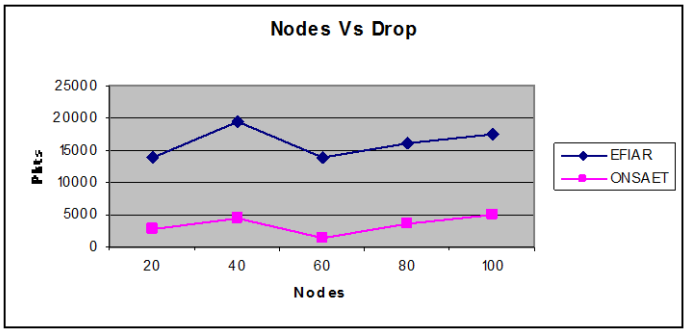

Fig 4: Nodes Vs Drop

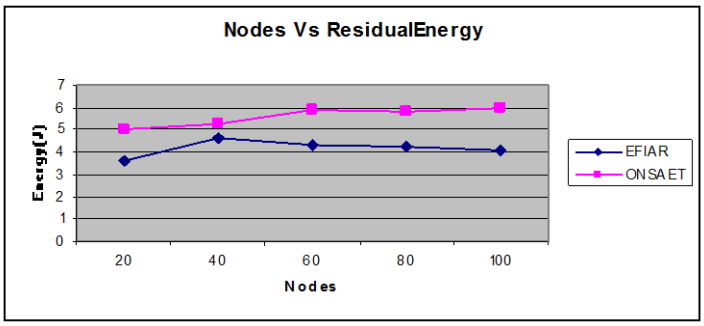

Fig 5: Nodes Vs Residual Energy

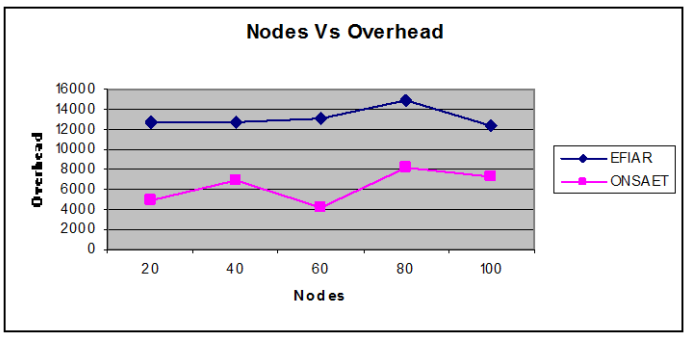

Fig 6: Nodes Vs Overhead

Figures 2 to 6 show the results of delay, delivery ratio, packet drop, residual energy and overhead by varying the number of nodes from 20 to 100 for the CBR traffic in ONSAET and EFIAR protocols. When comparing the performance of the two protocols, we infer that ONSAET outperforms EFIAR by 26% in terms of delay, 60% in terms of delivery ratio, 80% in terms of drop, 25% in terms of residual energy and 53% in terms of overhead.

B. Based on Attackers: In our simulation we vary the number of attackers as 1,2,3,4 and 5.

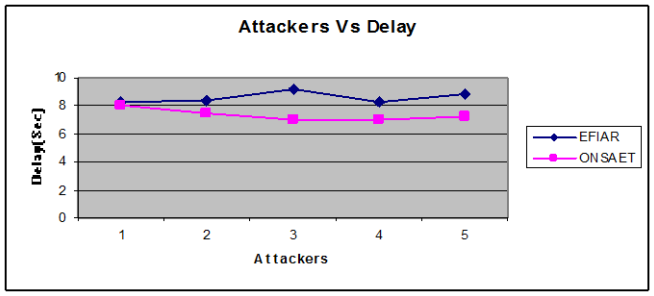

Fig 7: Attackers Vs Delay

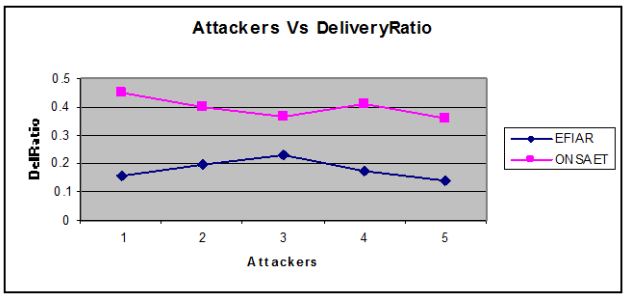

Fig 8: Attackers Vs Delivery Ratio

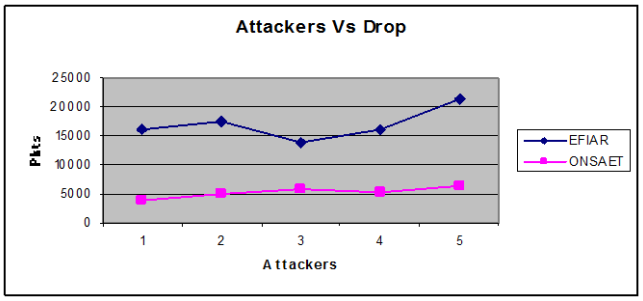

Fig 9: Attackers Vs Drop

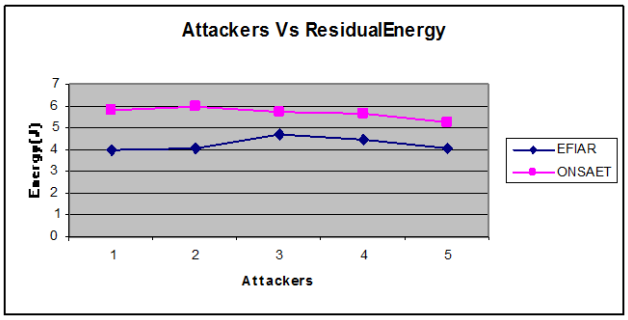

Fig 10: Attackers Vs Residual Energy

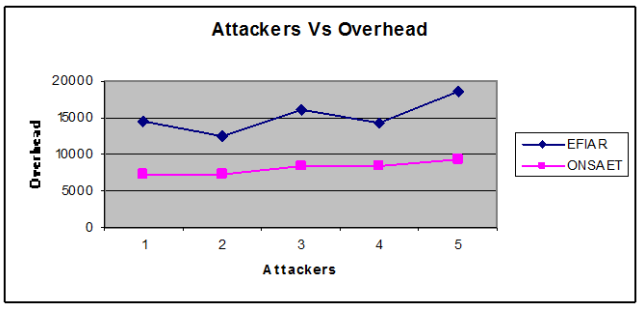

Fig 11: Attackers Vs Overhead

Figures 7 to 11 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 ONSAET and EFIAR protocols. When comparing the performance of the two protocols, we infer that ONSAET 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 a Optimal Node Selection and Alarm Exchange Technique for Reducing the Security Cost and False Positives 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 neighbour 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 through the nodes with minimum security costs. Thus, ensuring that the node selection process is optimal and also the security costs as well as the false alarms raised in the network is 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