NAODV-Distributed Packet Dropping Attack Detection in MANETs

Bobby Sharma Kakoty
Dept. of Computer Science & Engineering
School of Engineering
Tezpur University, Tezpur

S. M. Hazarika
Dept. of Computer Science & Engineering
School of Engineering
Tezpur University, Tezpur

N. Sarma
Dept. of Computer Science & Engineering
School of Engineering
Tezpur University, Tezpur

ABSTRACT
Mobile ad hoc network (MANET) is a self configuring network in which mobile nodes are connected by wireless link. Communication in MANET is done with the help of cooperation of nodes in the network. Due to its intrinsic properties like dynamic network topology, open medium, lack of central monitoring system, these are vulnerable to several attacks. Out of different attacks, packet dropping attack is considered as one of the serious threats as in this kind of attack, malicious node invariably drops the packets which are supposed to be forwarded to destination. Thus, it degrades network performance. In this paper, a distributed packet dropping attack (PDA) detection methodology named NAODV, is proposed. Detection and isolation of malicious node is based on cooperative participation of nodes involved in communication based on TRUST level of the nodes. TRUST levels of the nodes are dynamically updated based on their qualitative participation in detection of malicious nodes. Performance of this methodology is evaluated through simulation in different network scenarios and results are compared with two existing methodologies.

Keywords
MANET, PDA, distributed packet dropping attack, TRUST, CONFIDENCE, decision tree.

1. INTRODUCTION
MANET has become a new paradigm for mobile hosts to adopt a network and to communicate without expecting an infrastructure. This leads the network nodes to depend on the co-operation of neighbor nodes [1][2][3][4]. The flexibility and adaptability of the network, which are the strength of MANETs, leads to several attacks [1][2]. These may include various Denial-of-Service (DoS) attack, impersonate-on, passive eaves dropping attack, active interfering etc. Moreover, uncooperative nodes in MANETs lead to security treats. Noncooperation of nodes may occur in two ways, either because of malicious node or because of selfish node [3]. Malicious nodes are categorized as faulty because they intentionally attack the system by dropping packets [5]. When an intruder attacks, it effects the entire network in various network performance parameters such as packet delivery ratio, throughput, end-to-end delay, network routing load and round trip time [10].

Packet dropping attack can be considered as the most vulnerable attack. Malicious node in the network drops packets intentionally which are supposed to be forwarded to reach destination [6][7][8][9] [12][13] [15][16]. Routes that pass through such kind of nodes fail to establish path from source to destination [8]. As a result, network performance degrades abruptly. Even it leads to complete failure of network.

A distributed PDA detection methodology is proposed. PDA is detected and confirmed not only by the node which has been suffering but also confirmed by other nodes in the network.

2. RELATED WORKS
In [14], authors use the idea of taking the nodes which are adjacent to data communication route to monitor the message forwarding behavior of the nodes en route. Packet dropping attack is addressed by post routing detection. Whenever it finds any abnormality, immediately it issues alarm packet to the source node. The main principle behind this algorithm is to use a set of neighbors for every node to work as observer to observe the packet forwarding behavior of the node under the route.

A distributed PDA detection approach, based on end-to-end connection is proposed in [22]. This detection and isolation mechanism of packet dropping attacker is based on three ID messages like path validation message (PVM) that enables E2E feedback loop between the source and the destination, attacker finder message (AFM) which will find the attacker node from the routing path and attacker isolation message (AIM) is used to isolate the attacker from routing path and updates the black list and then triggers to neighbors with updated information. Another cooperative PDA detection mechanism has been proposed in [23], which is based on cooperative participation of nodes in MANETs. It is a collaborative distributed protocol which involves cryptographic key distribution and intrusion detection activity for detection of malicious packet dropping attack. Key distribution requires a trust management scheme to dynamically bind the trust relationship between the key distribution servers and the clients. Initial security to intrusion detection mechanism is provided by LLCs (location limited side channels). then it provides a dynamic trust management scheme for key distribution which leads to dynamic trust management scheme. A reputation based approach to detect and isolate the misbehaving nodes has been proposed in [24], which can be integrated with source routing protocol. It is based on sending acknowledgement packets and counting the data packets on an active path. It has basic three steps like detection of malicious group, identification of particular misbehaving node, isolation and mitigation of misbehaving node. A solution is proposed in [25] to monitor, detect and isolate misbehaving nodes that involves in packet dropping attack. It suggests a social-based approach to approve detection and isolation of malicious nodes to reduce false positive rate of detection. This methodology is failed to analyze collusive dropping of packets. It has some limitations to handle continuous packet dropping as well as detection of selective misbehavior. In such situation detection is delayed because of Bayesian approach for judgment. A novel simplified IDS for detecting packet dropping attack in MANET is proposed in [26]. Here mobility aspects is considered explicitly by means of a heuristics which considers the forwarding operation at node. In [27], a homographic linear authenticator based public auditing architecture is proposed which assist the packet dropping attack detector to detect the attack accurately by verifying the truthfulness of packet loss information reported by nodes. So, correlation between loss packets is established.

3. PROPOSED METHODOLOGY

3.1 Assumption

In the system model, low rates of packet loss or any other packets drop other than malicious packet drop are assumed as *threshold* packet drop. When packet drop is more than the threshold packet drop than PDA is suspected. PDA is suspected in certain node based on the different network performance parameters such as packet delivery ratio as well as throughput of the network. It is assumed that packets are forwarded in a hop-by-hop fashion in on demand ad hoc way. The communication links are assumed to be bi-directional and there is no wireless channel error. All nodes use unidirectional antennas for bidirectional communications. Neighbor discovery protocol is assumed to be worked in such a way that every node can understand its corresponding neighbor.

It is assumed that all the nodes in MANET have the capability to understand packet drop in them. Thus it has the ability to understand the threshold packet drop as well as malicious packet drop. Promiscuous mode of node is enabled with source routing. A malicious node can drop packets continuously or selectively. Here collusion of more than one node is not considered so that malicious node can monitor each other and collude and mask the misbehavior of each other.

We assume that intelligent agent are supposed to adapt decision making by the cooperation with other nodes in the communication. Activity of the agent is dependent on the network performance matrices such as:

a. Delay in Delivery of the Packet
b. Response Time
c. Quality of Service Provider
d. Packet Forwarding Misbehavior

Accordingly in every node, local agent calculates the following to suspect packet drop misbehavior i.e.:

$$\text{Packet Drop Ratio (PDR)} = \frac{\sum \text{No.of packets received}}{\sum \text{No.of packets sent}}$$

$$\text{Throughput} = \frac{y}{t}$$ i.e. y numbers of packets are delivered within t times at a node.

If for a particular node PDR is very high and throughput is very low then that node is suspected of malicious activity. It is assumed that nodes are communicating to one another in wireless channel and there is some amount of packet drop due to congestion, overload or for media interference. Flow of traffic will be observed by each node that participated in communication. Agents will perform Local analysis of packet drop in every node.

3.2 System Architecture

Proposed distributed PDA detection methodology is based on cooperation of different nodes. Data, collected from different nodes are analyzed to detect PDA. Upon detection, message will be distributed amongst the nodes in terms of alarm to avoid the malicious nodes for packet forwarding. The entire system is an automatic, self manageable process. Data, collected from various node's host level audit system like "system log", are analyzed by the system. Then data abstraction is done on the collected data. As shown in Fig 1, different modules and their functions are discussed as follows:

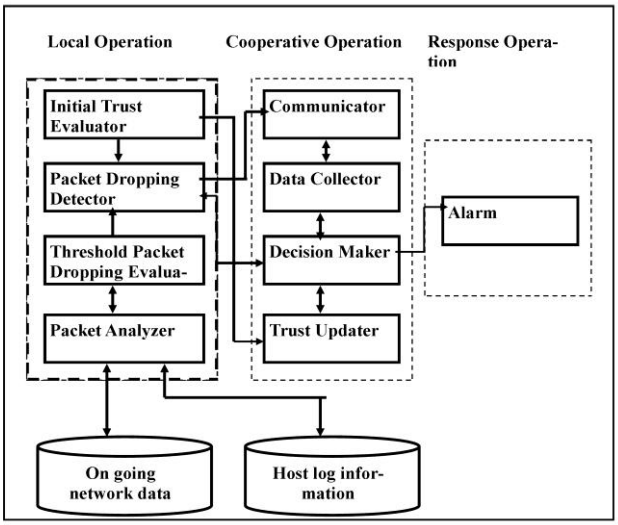

Fig 1: Schematic diagram of distributed PDA detection methodology

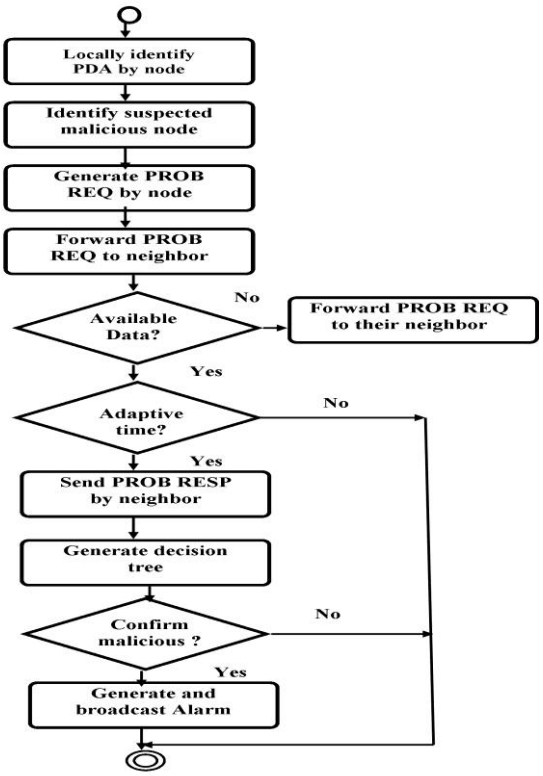

Fig 2: Activity diagram of NAODV

3.2.1 Local agent. Local agent runs on each node to detect PDA locally. Then these agents will collaborate with other agent to confirm PDA in the network.

3.2.1.1 Packet analyzer: It analyzes the packet stream with various fields in the packets and stores the content according to the specified logic. This network analyzer will legitimately be used to analyze each packet that comes to every node to identify any suspected malicious packet drop in the network.

3.2.1.2 Threshold packet drop evaluator: It determines the threshold value of packet drop due to any reason except malicious packet dropping.

3.2.1.3 Initial trust evaluator: When a node first time joins the network, its trust value is evaluated by this agent in cooperation with neighbor nodes.

3.2.1.4 Packet drop detector: It compares the dropped packets that are evaluated by packet analyzer with threshold packet drop. Once the number of dropped packets are more than the threshold packet drop then it communicates to cooperative agent
for identification of malicious packet drop.

3.2.2 Cooperative agent

3.2.2.1Communicator: If the local agent "packet drop detector" finds excessive packet drop which is more than the threshold packet drop due to some suspected malicious node, this module activates and it sends the PROB REQ message to all its neighbors to know TRUST and CONFIDENCE level of the suspected malicious node within the adaptive time. While sending
PROB REQ, it takes care to avoid feed back or to receive duplicate
packets.

3.2.2.2 Data collector: PROB RESP, which are sent in response to PROB REQ are collected by this module within the adaptive time. Adaptive time is based on either of the following conditions, randomly generating the options:

a. Number of node scanned (% of total nodes)
b. Number of Responses expected(% of total nodes)
c. Fixed amount of time to forward PROB REQ and to get PROB RESP
d. Number of level crossed

3.2.2.3 Decision Maker: PROB RESP that is collected from various neighbor containing TRUST and CONFIDENCE level of suspected malicious node, are analyzed to confirm whether the suspected malicious node is really a malicious node or not. For this incremental decision tree algorithm ID5R [18][19][20][21] is used.

3.2.2.4 Trust updater: It dynamically updates the TRUST level TL_c of a node based on decision generated by the decision maker.

a. For a node, TL_c is TRUST level of the node and TRUST level sent by the node for suspected malicious node is TL_m.
b. Find global decision GD from "Decision Maker" for suspected malicious node.
c. If (GD="malicious")
If TL_m=high
TL_c="low";
else
TL_c=high;
If (GD="not malicious")
If TL_m=high
TL_c="low";
else
TL_c=high;

3.2.3.Response agent

3.2.3.1 Alarm generator: If the "Decision Maker" decides that suspected malicious node is a confirmed malicious node then alarm will be broadcasted in the network to avoid the malicious node for packet forwarding.

4. EXPERIMENTAL STUDIES

4.1 Simulation Environment

The performance of the proposed methodology has been evaluated for different network environments in NS 2 (Network Simulator version 2). Simulation environment is considered as given in Table 1.

Table 1. Simulation Environment

Animation area	1000m X 1000m
Mobility model	Random way point
Channel type	Wireless
No. of nodes	100
Simulation time	600 sec
Pause time	10-70 sec
Node Speed	10-70 m/s
Data rate	100 kbs
Wireless	100 m
Packet size	512 byte
Traffic type	CBR
Routing protocol	AODV

Network performance is evaluated based on the following network performance parameters.

Detection rate: Detection rate is a factor which is used to determine the efficiency of the methodology to determine packet dropping attack. It can be calculated by the following formulae,

Detection rate =(Number of true positive)/(Number of true positive + number of false negatives)

False positive rate: It is measured as percentage of the ratio of total number of genuine nodes but detected as malicious nodes to Total number of genuine nodes.

$$FPR=\frac{\text{Total number of genuine nodes but detected as malicious nodes}}{\text{Total number of genuine nodes.}}X\ 100$$

Throughput of the network: It is measured as bits per sec. It can be calculated by number of packets delivered per time slot.

Throughput= (Total number of delivered data packets/Total simulation time)

Packet Delivery Ratio (PDR): It is determined as the ratio between the numbers of packets received by the destination to the number packets originated by the application i.e. sent from the source to destination.

Proposed algorithm, NAODV, is compared with SAODV (Secure Ad hoc on demand distance vector) proposed in [30][32][33]-[34][35][36] and TAODV (Trusted Ad hoc on demand distance vector) [31][37]. SAODV routing protocol is an extension of the AODV routing protocol that can be used to protect the route discovery mechanism providing security features like integrity and authentication. It uses the cryptographic method to secure AODV protocol. TAODV is a

secure routing protocol which is an extension of AODV protocol. It is based on trust model. It uses trust relationship among the nodes for routing. It employs a trust model derived from subjective logic. In this protocol, signing and verification of digital signature at each routing message is not required

4.2 Results and discussion

4.2.1 Detection rate

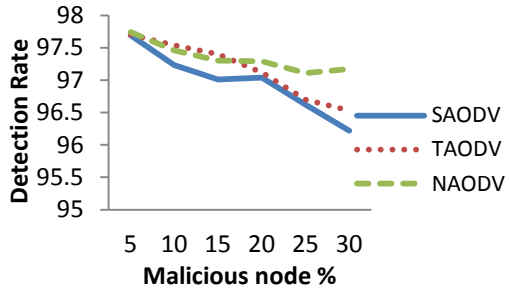

Fig 3: Percentage of malicious node vs. detection rate

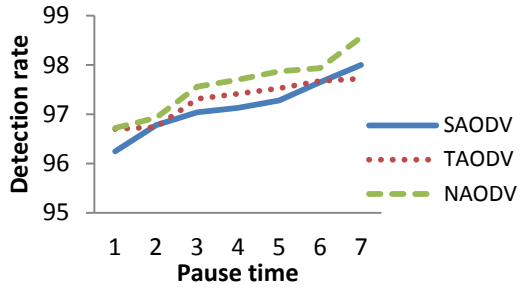

Fig 4: Pause time vs. detection rate

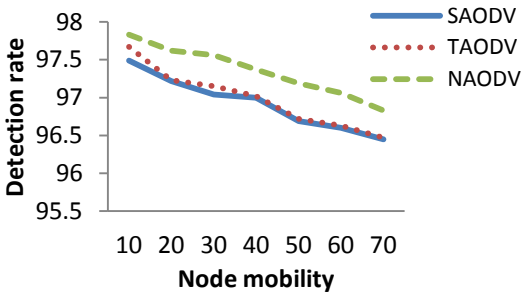

Fig 5: Node mobility vs. detection rate

Fig 3 shows the detection rate of all the three different methodologies with increased number malicious nodes. Similarly, Fig 4 shows the detection rate with increased pause time, while Fig 5 shows the detection rate with increased node mobility. It is observed that NAODV shows the best performance in all the three cases.

It can be explained by the fact that in NAODV, malicious node detection and avoidance is completely based on cooperation of neighbors. Global decision is taken based on decision tree algorithm. Accordingly TRUST level of the node is dynamically updated. On the other hand, TAODV is a trusted routing protocol that cooperates with a self organized key management mechanism. Moreover it performs trusted routing in a self-organized way. In SAODV, signature is verified by both source node and intermediate node and then only routing table will be updated. Malicious node cannot generate signature of destination node, hence it will not be able to impersonate destination node.

4.2.2 False positive rate

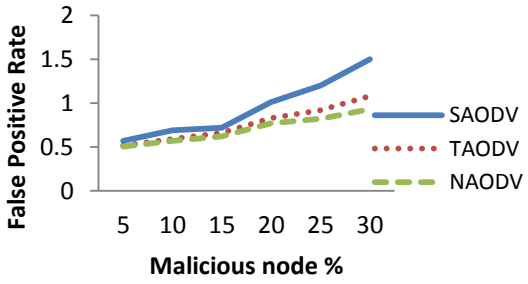

Fig 6: Percentage of malicious node vs. false positive rate

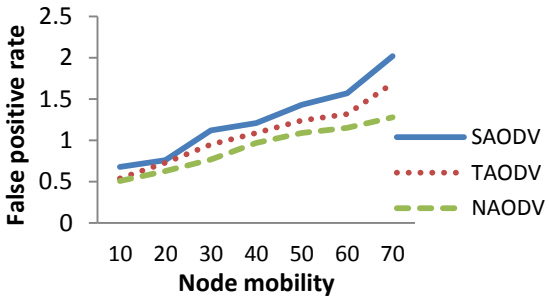

Fig 7: Node mobility vs. false positive rate

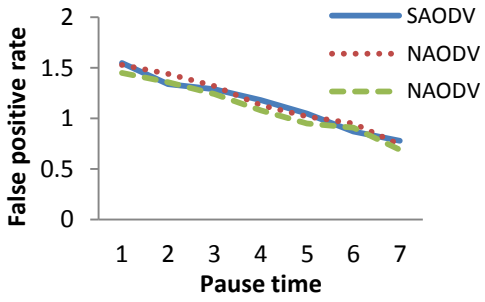

Fig 8: Pause time vs. false positive rate

Fig 6, Fig 7 and Fig 8 compare the false positive rate of three different methodologies with respect to increased number of malicious node, increased node mobility and increased pause time. SAODV is not designed to resist the DoS attack like packet dropping attack. It provides a cryptographic support to secure the routing protocol. It shows the vulnerabilities to packet drop attack. Similarly TAODV is also dedicated for trusted routing, not directly involve with PDA detection. On the other hand, in NAODV, detection of malicious packet dropping is done in distributed co-operative way and after confirmation only it will generate an alarm to avoid the malicious nodes for further packet forwarding, hence false positive rate will be comparatively less.

4.2.3 Packet delivery ratio

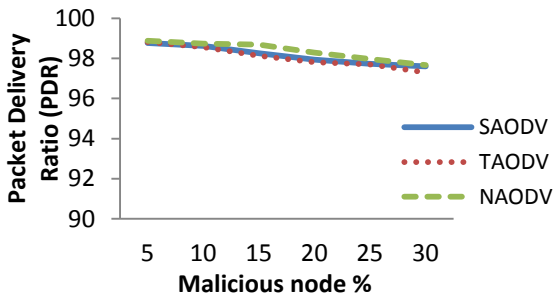

Fig 9: Percentage of malicious node vs. PDR

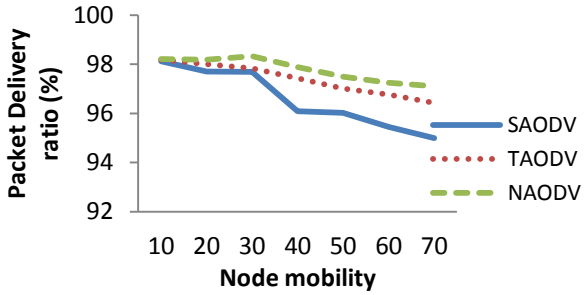

Fig 10: Node mobility vs. PDR

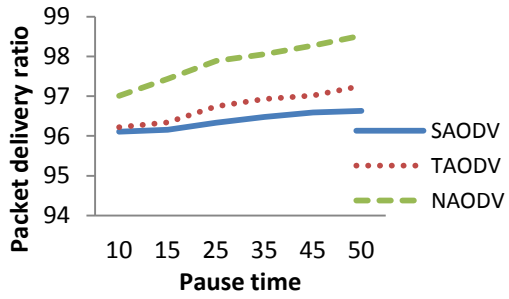

Fig 11: Pause time vs. PDR

Fig 9, Fig 10 and Fig 11, compare the packet delivery ratio of the three methodologies. In all the three cases, TAODV performs the best. TAODV is simply meant for packet dropping attack detection. So, for any network condition, it tries to detect malicious node in distributed cooperative way and avoid the same for packet forwarding. If the packet drop ratio is decreasing, then oppositely packet delivery ratio will be increasing.

When the node mobility is higher, it signifies the high failure of connectivity and frequent change of topology. As a result, number of packets drop will be more. Nodes may be falsely accused of malicious. It is more in case of SAODV than TAODV, while less in case of NAODV. SAODV chooses the safest path instead of shortest path and tries to eliminate the malicious nodes in the way, so the average path length is longer. But when the node mobility is higher, the network topology will break frequently and it will not be able to deliver the packets on time. Moreover high security application of SAODV will resist the path more.

4.2.4 Throughput

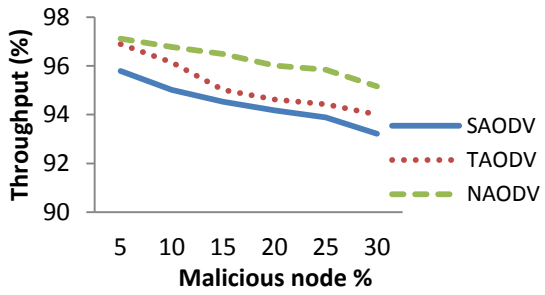

Fig 12: Percentage of malicious node vs. Throughput

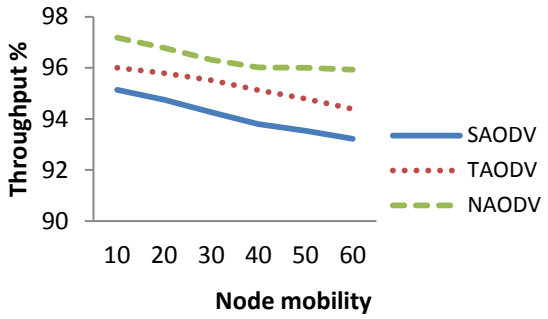

Fig 13: Node mobility vs. throughput

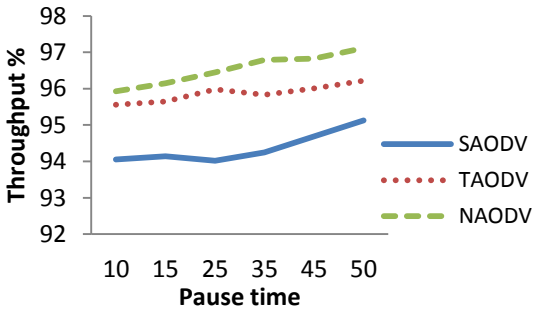

Fig 14: Pause time vs. throughput

Throughput of the network is compared for three methodologies shown in Fig.12, Fig.13 and Fig.14. NAODV shows best performance. In SAODV, it takes some extra time for computation and verification of security fields during route discovery process. Moreover it always prefers safest path instead of shortest path. These all consume some extra time. Since throughput depends on total number of packets delivered in specified time, hence it will come down. In TAODV also consumes extra time for TRUST updation by evidence & opinion, exchange and authentication. On the other hand NAODV doesn't consume much time for route discovery and there is not so complex security measures during route discovery so it delivers more packets in specified time. This implies more throughputs.

5. CONCLUSIONS

PDA detection in MANET is a very challenging task due to dynamic nature of the network. Due to node mobility, there is a lack of central point from where traffic can be observed. Centralized packet dropping attack detection methodology is not suitable because of its static nature of detection in a dynamic

network. So, distributed packet dropping attack detection methodology has the potential to be preferred. PDA in a node is to be confirmed not only by the node itself but also to be confirmed by the various neighbors of the node. Once detected, malicious nodes are avoided from packet forwarding by the network. TRUST and CONFIDENCE level computation of nodes in MANET is a challenging task. Untrusted node wreaks PDA more and thus performance degrades abruptly. Trustable node gives more CONFIDENCE to the network. The proposed methodology has been experimented in various networks settings with various parameters. The respective results are compared with two existing systems and analyzed. This methodology doesn't consider the collaborative malicious packet dropping attack and battery power consumption. Moreover, condition of "No response" are not analyzed.

6. REFERENCES

[1] D. Sterne, P. Balasubramanyam, D. Carman, B. Wilson, R. Talpade, C. Ko,R. Balupari, C-Y. Tseng, T. Bowen, K. Levitt and J. Rowe, "A General Cooperative Intrusion Detection Architecture for MANETs", Proceedings of the Third IEEE International Workshop on Information Assurance, IEEE Computer Society Washington, DC, USA ©2005, Pages 57-70, ISBN:0-7695-2317-X

[2] Giovanni Vigna, Sumit Gwalani, Kavitha Srinivasan, Elizabeth M. Belding-Royer, Richard A. Kemmerer, "An Intrusion Detection Tool for AODV-basedAdhocWirelessNetworks", Computer Security Applica-ions Conference 2004,Page(s):16 27, ISSN : 1063-9527, Print ISBN:0-7695-2252-1

[3] Jaydip Sen, "A Distributed Trust Management Framework for Detecting Malicious Packet Dropping Nodes In A Mobile Adhoc Network", International Journal of Network Security & Its Applications (IJNSA) 2010, Vol.2, No.4

[4] Chin- Yang Henry Tseng, "Distributed Intrusion Detection Models for Mobile AdHoc Networks", DISSERTATI on Submitted in partial satisfaction of the requirements for the degree of Doctor Of Philosophy in Computer Science in the office of graduate studies of the University of California Davis

[5] Alper Tugay M ızrak, Yu -Chung Ch eng, Keith Marzullo and Stefan Savage, "Faith: Detecting and Isolating Malicious Routers", IEEE Transactions On Dependable And Secure Computing 2006, VOL. 3, NO. 3

[6] A.Rajaram and Dr. S. Palaniswami, "Malicious Node Detection System for Mobile Ad hoc Networks", (IJCSIT) International Journal of Computer Science and Information

[7] Technologies, 2010,Vol.1, no. 2 , pages:77-85

[8] Muhammad Zeshan, Shoab A.Khan, Ahmad Raza Cheema and Attique Ahmed ,"Adding Security against Packet Dropping Attack in Mobile Ad hoc Networks", Future Information Technology and Management Engineering, 2008. FITME '08. International Seminar(2008 IEEE), Page(s):568 –

[9] 572, Print ISBN:978-0-7695-3480-0

[10] Soufiene Djahel, Farid Nat-abdesselam and Zonghua Zhang,"Mitigating Packet Dropping Problem in Mobile AdHoc Networks: Proposals and Challenges", IEEE communications surveys & tutorials(2011), vol. 13, No. 4

[11] Julian Benadit.P, Sharmila Baskaran and Ramya Taimanessamy, "Detecting Malicious Packet Dropping Using Statistical Traffic Patterns", IJCSI International Journal of Computer Science Issues(2011), Vol.8, Issue 3, No. 2, ISSN (Online): 1694-0814

[12] V. Madhu Viswanatham and A.A. Chari, "An Approach for Detecting Attacks in Mobile Adhoc Networks", Journal of Computer Science 2008, Volume 4, Issue 3, Pages 245-251

[13] Ricardo Puttini, Jean-Marc Percher, Ludovic Mé and Rafael de Sousa, "A Fully Distributed IDS for MANET", Computers and Communications, 2004. Proceedings. ISCC 2004. Vol. 1, Page(s): 331 – 338, Print ISBN: 0-7803-8623-X

[14] Tanapat Anusas-amornkul, "On Detection Mechanisms and Their Performance for Packet Dropping Attack in Ad Hoc Networks", Submitted to the Graduate Faculty of the School of Information Sciences in partial fulfillment of the requirements for the degree of Doctor of Philosophy University of Pittsburgh 2008

[15] Shukla Banerjee, "Detection/Removal of Cooperative Black and Gray Hole Attack in Mobile Ad-Hoc Networks," Proceedings of the World Congress on Engineering and Computer Science 2008, USA

[16] Xu Li, Rongxing Lu, Xiaohui Liang, and Xuemin (Sherman) Shen, "Side Channel Monitoring: Packet Drop Attack Detection in Wireless Ad Hoc Networks", Communications (ICC), 2011 IEEE International Conference, Page(s): 1-5, ISSN : 1550-3607, E-ISBN :978-1-61284-231-8, Print ISBN: 978-1-61284-232-5

[17] Aikaterini Mitrokotsa, Rosa Mavropodi, Christos Douligeris, "Intrusion Detection of Packet Dropping Attacksin Mobile AdHoc Networks", Ayia Napa, Cyprus, July 6-7, 2006

[18] Jaydip Sen, M. Girish Chandra, P. Balamuralidhar, Harihara S.G., Harish Reddy, "A Distributed Protocol for Detection of Packet Dropping Attack in Mobile Ad Hoc Networks", Telecommunic-ations and Malaysia International Conference on Communications, 2007. ICT-MICC 2007. IEEE International Conference, Page(s):75 – 80, E-ISBN :978-1-4244-1094-1,Print ISBN:978-1-4244-1094-1

[19] Aishwarya Sagar Anand Ukey, Meenu Chawla, "Detection of Packet Dropping Attack Using Improved Acknowledgement Based Scheme in MANET", IJCSI International Journal of Computer Science Issues, Vol. 7, Issue 4, No 1, July 2010 ISSN (Online): 1694-0784 ISSN (Print): 1694-0814

[20] P.E. Utgoff, "Incremental Induction of Decision Trees", Machine Learning, Vol.4, No.2, pages:161-186, 1989.

[21] Dimitrios Kalles and Tim M Orris, " Efficient Incremental Induction of Decision Tree", Machine Learning, 1 , 1{13 (1995) 1995 Kluwer Academic Publishers, Boston. Manufactured in T he Netherlands

[22] Ding-An Chiang, Wei Chen, Yi-Fan Wang And Lain-Jinn Hwang, "Rules Generation From the Decision Tree", Journal of Information Science and Engineering 17, 325-339 (2001)

[23] Sam Chao, Fai Wong, "An Incremental Decision Tree Learning Methodology Regarding Attributes In Medical Data Mining", Machine Learning and Cybernetics, 2009

International Conference, Page(s):1694 – 1699, E-ISBN :978-1-4244-3703-0, Print ISBN:978-1-4244-3702-3

[24] Ahmed Mohamed Abdalla, Ahmad H. Almazeed, Imane Aly Saroit and Amira Kotb "Detection and Isolation of Packet Dropping Attacker in MANETs ", (IJACSA) International Journal of Advanced Computer Science and Applications 2013, Vol. 4, No.4

[25] Jaydip Sen, M. Girish Chandra, P. Balamuralidhar, Harihara S.G. and Harish Reddy, "A Distributed Protocol for Detection of Packet Dropping Attack in Mobile Ad Hoc Networks", Telecommunications and Malaysia International Conference on Communications, 2007. ICT-MICC 2007. IEEE International Conference, Page(s):75 – 80, E-ISBN :978-1-4244-1094-1, Print ISBN:978-1-4244-1094-1

[26] Aishwarya Sagar Anand Ukey and Meenu Chawla, "Detection of Packet Dropping Attack Using Improved Acknowledgement Based Scheme in MANET", IJCSI International Journal of Computer Science Issues 2010, Vol. 7, Issue 4, No 1, ISSN (Online): 1694-0784, ISSN (Print): 1694-0814

[27] Djamel Djenouri and Nadjib Badache, "On eliminating packet droppers in MANET: A modular solution", Elsevier, AdHoc Networks (2009), Volume 7 Issue 6, Pages 1243-1258

[28] Leovigildo Sánchez-Casado, Gabriel Mací-Fernández and Pedro Garcia-Teodoro "An Efficient Cross-Layer Approach for Malicious Packet Dropping Detection in MANETs", Proceedings of the 2012 IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications, Pages 231-238, ISBN: 978-0-7695-4745-9

[29] Tao Shu and Marwan Krunz "Detection of malicious packet dropping in wireless ad hoc networks based on privacy-preserving public auditing", Proceedings of the fifth ACM conference on Security and Privacy in Wireless and Mobile Networks 2012, Pages 87-98, ISBN: 978-1-4503-1265-3

[30] S.Madhavi, K.Duraiswamy, B.Kalaavathi and S.Vijayaragavan, "Performance Analysis of SAODV with DOS Attack", International Journal of Electronics Communication and Computer Engineering, Vol 3, Issue 2, ISSN 2249 –071X

[31] Xiaoqi Li, Michael R. Lyu and Jiangchuan Liu, "A Trust Model Based Routing Protocol for Secure Ad Hoc Networks", Aerospace Conference, 2004. Proceedings. 2004 IEEE, Vol.2, Page(s):1286 – 1295, ISSN :1095-323X, Print ISBN:0-7803-8155-6

[32] S.Madhavi, K.Duraiswamy, B.Kalaavathi and S.Vijayaragavan, "Performance Analysis of SAODV with DOS Attack", International Journal of Electronics Communication and Computer Engineering, Vol 3, Issue 2, ISSN 2249 –071X

[33] Xiaoqi Li, Michael R. Lyu and Jiangchuan Liu, "A Trust Model Based Routing Protocol for Secure Ad Hoc Networks", Aerospace Conference, 2004. Proceedings. 2004 IEEE, Vol.2, Page(s):1286 – 1295, ISSN :1095-323X, Print ISBN:0-7803-8155-6

[34] R.Balakrishna, U.Rajeswar Rao , Dr.Geethanjali and M.S.Bhagyashekar, "Comparisons of SAODV and TAODV, DSR Mobile ad hoc network Routing Protocols", Int. J. Advanced Networking and Applications 445 2010, Vol- 02, Issue: 01 Pages: 445-451 (2010)

[35] S.Madhavi K.Duraiswamy B.Kalaavathi S and Vijayaragavan, "Performance Analysis of SAODV with DOS Attac", International Journal of Electronics Communication and Computer Engineering, Volume 3, Issue 2, ISSN 2249 –071X

[36] Latha Tamilselvan and Dr. V. Sankaranarayanan↑, "Prevention of Impersonation Attack in Wireless Mobile Ad hoc Networks," IJCSNS International Journal of Computer Science and Network Security 2007, VOL.7 No.3

[37] Er. Gurjeet Singh, "Performance and Effectiveness of Secure Routing Protocol in Manet", Global journal of computer science and technology 2012, Volume 12 Issue 5

[38] Yuxia Lin, A. Hamed Mohsenian Rad, Vincent W.S. Wong and Joo-Han Song, "Experimental Comparisons between SAODV and AODV Routing Protocols", WMuNeP'05.

[39] Mrs. P.Vigneswari, R.Anusha, D.Preethi, R.Jayashree, V.Nandhini, Comparative Analysis of and Trusted AODV (TAODV) in MANET", International Journal of Advanced Information Science and Technology (IJAIST) 2013, ISSN: 2319:2682 Vol.10, No.10