IJARCCE

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

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 10, October 2017

An Adaptive and Collaborative Enhanced Trust Based Intrusion Detection System MANET

Pooja Malviya[1], Vivek Sharma[2]

M. Tech Research Scholar, SATI Vidisha (M.P), India [1]

Assistant Professor, SATI Vidisha (M.P), India [2]

Abstract: MANET provides a flexible framework for the wireless communication which does not requires infrastructure or centralized controlling, because of the these abilities the MANET has great applicability in the applications where the other system cannot be deployed such as remote sensing, disaster management and military applications. However such flexibility comes with the cost of a number of limitations which can be exploited to compromise the security of the system. This paper we are presents an adaptive and enhanced trust based mechanism to detect and remove the malicious nodes from the network. In the proposed technique each node observes the packets transmission around it, and analyse it on the bases of trust estimation function which relates the RREQ, RREP and DATA packets. Furthermore these individual trust ratings are shared with other nodes to make it a collaborative system which provides much reliable detection of malicious nodes and minimizes the false detection probabilities. The proposed technique can also be integrated into MANET protocols with minimum efforts and it also have minimal impact of traffic overheads. The experimental result verifies that the proposed technique can successfully counter the black hole attack, selfish attack, collaborative attacks etc.

Keywords: Intrusion detection technique (IDS), Mobile Ad-Hoc Network (MANET).

I. INTRODUCTION

Mobile Ad-Hoc Network (MANET) is considered as a group of mobile nodes capable to communicate with each other's using a wireless communication links without any centralized controlling (managing) infrastructure. Considering the fact that the system can consist a large number of mobile nodes, the network may lead to continuously changing and complex topologies. The functionality of MANET such as routing, multi hop packet forwarding etc. depends upon collaborative behavior from each and every node in the network [8]. This collaboration among the nodes is the fundamental requirement for the MANET, and so it has the great impact on its performance. MANET is continuously gaining applicability in diverse fields like remote sensing, military and industrial applications, disaster management etc. [8].

Besides being useful in a number of applications the MANETs due to their nature are more vulnerable to security attacks than other centralized networks. Security in wireless ad hoc networks is difficult because of the limited physical access of nodes, the irregular connectivity characteristics, lack of centralized monitoring, controlling and certification authority. In comparison to the wired networks where an intruder must gain either direct physical access to the network or required to bypass several layers of protection like firewalls and gateways, intruder in a MANET can approach at any node directly or indirectly the condition get further worse when intrusion is done by a compromised node within the network. Hence every node must be capable for handing directly or indirectly attacks.

The structure of MANETs present a number of challenges for Intrusion Detection Systems (IDS). Monitoring the data transmitted by all the nodes with limited power makes it difficult to implement IDS on MANETS. Mobility of nodes and dynamic topological changes also imposes complexity in observations and hence on IDS. In this paper, we proposed an Adaptive and Collaborative Enhanced Trust Based Intrusion Detection System for MANETs.

The Rest of the paper is arranged as the section 2 presents a review on the related work. The section 3 introduces the various type of attack the proposed technique can overcome. Section 4 describes the proposed work in detail. Section 5 the simulation results are presents, and finally section 6 presents the concluding remarks with future work.

II. RELATED WORK

As the problem with the MANET security is not hidden and therefore a number of approach related to IDS has been already proposed. This section reviews the approached most relevant to our work.

IJARCCE

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

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 10, October 2017

#The Adaptive Three ACKnowledgements (A3ACKs) [1]scheme for preventing limited transmission power [1], receiver collision [1][5] and collaborative attacks (collusion attack) [4][1]in Mobile Ad-Hoc Networks. The A3ACK scheme implies three different type of acknowledgment modes with three different types of ACK packets as listed in table 1.

Table 1: Packet Typesin A3ACK Scheme.

Packet Type	AACK	TACK	THACK
Packet ID	1	2	3

named as AACK, TACK (Two-ACK) and THACK (Three-ACK) packets, as the name suggest they are used to acknowledge the forwarder node, node one behind the actual packed forwarder node(or two hops) away, andnode two behind the actual packed forwarder node (or three hops)away. All in the direction opposite to that of data packets.

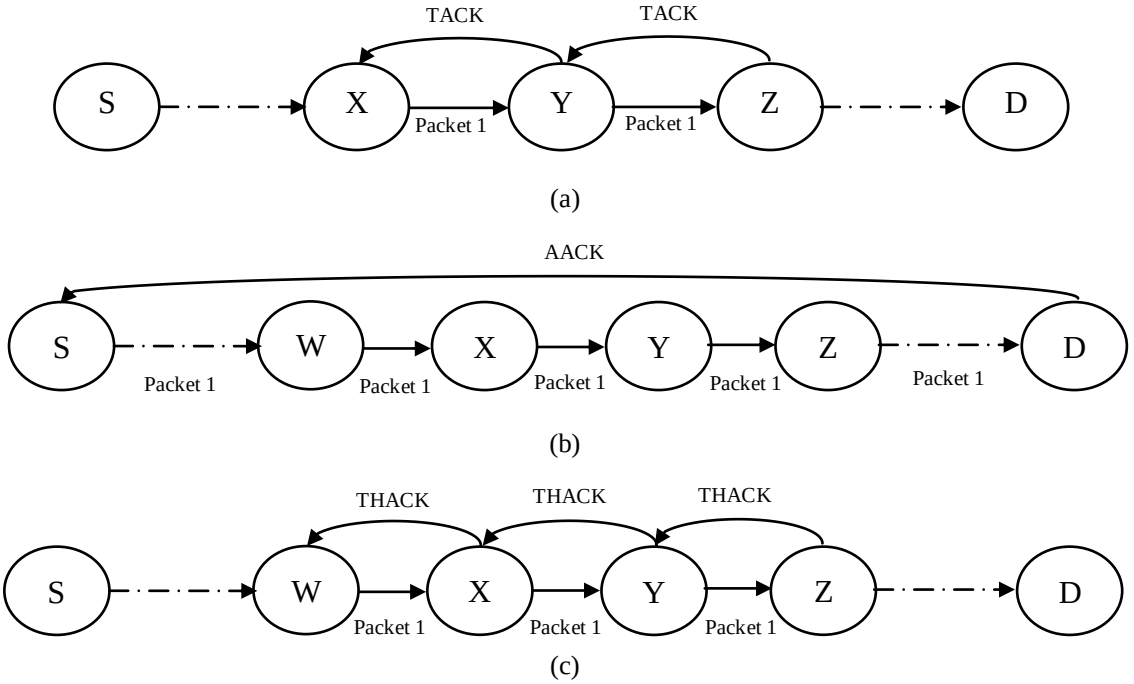

Figure 1: Illustration of AACK (a), TWOACK (b) and A3ACK (c) technique.

The A3ACK scheme is based on AACK [2] where the AACK is based on TWOACK [3] hence to better understand let start with the TWOACK technique consider the figure 1 let the Route Discovery has already doneand a route [S →···→W →X→Y→Z→···→ D] from source node S to destination node D has been discovered.Through this route when X forwards a data packet to Y, then Y must forward that packet to Z, but there has no way, that X can know, if the packet forwarded to Z successfully or not. Hence if Y is a malicious node and is not forwarding the packet to Z there is no way to detect it.

The TWOACK technique is designed to overcome this problem: consider the figure 1 when Z receives a data packet, it sends a TWOACK packet to X which positioned over two hops back, this TWOACK packet notifies X that the data packet has successfully reached to Z. Every node in the route will follow the similar procedure except the node first hop away from the source.

However in case if node X does not detect the TWOACK packet then it may consider that either the node Y is not forwarding or the Z is not replying, so the X can only detect that the link from Y →Z is misbehaving. Such nodes (link) will not be chosen during the route selection for data transmission later on.

The TWOACK technique is useful in detection of independent misbehaving nodes but will not work with collaborative attacks. It also increases the traffic overhead however this can be reduced by using S-TWOACK (Selective-TWOACK). Furthermore this technique can only detect misbehaving links not the node so the node may still exist in the network.

To overcome the limitation of TWOACK the AACK scheme was proposed this scheme may be considered as a hybrid of an Enhanced-TWOACK (E-TWOACK) scheme and an end-to-end acknowledgment scheme. It overcomes the first limitation of TWOACK by reducing the routing overhead by utilizing the end-to-end acknowledgment scheme which

IJARCCE

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

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 10, October 2017

reduces the overhead traffic of TWOACK scheme, with paths more than two hops, by a factor of (number of hops-2) per one data packet. The second limitation of TWOACK is overcome by enhancement in the calculation part of the TWOACK scheme which makes it capable of node detection instead of link detection.The AACK scheme overcomes two (limited transmission power and receiver collision) of the three attacks stated initially. However it fails in detection of collaborative attack especially when two consecutive collaborative misbehaving nodes occurs in a route.

To overcome the limitation of AACK the A3ACK scheme was proposed. In A3ACK the default model is AACK model as shown in figure 1(b), where the node S sends data packet to node D through the active route that it gets from DSR routing protocol. When destination D receives the sending data packet, it generates an AACK packet and sends back to the S node using the same route path. If the node S didn't receive the AACK packet within predefined time, it switches to E-TWOACK model to detect any misbehaving nodes in same route. If the node S further fails to receive TACK packet within a predefined time, it finally switches to THACK model to detect any collaborative misbehaving nodes in the route path. The THACK model aims to overcomeall three problemseven with the presence of two consecutive misbehaving nodes in a route path.

III. COLLABORATIVE ATACKS IN MANET

A collaborative attack in MANET is a kind of homogeneous attack (i.e. blackhole or wormhole attack) which involvest Two or more colluding nodes [4]. It is classified as internal active attack that can be triggered by single or multiple attackers. It is also referred as the first level of attack, in which the attackeris only interested in disrupting the foundation mechanism of the network.

A. Direct Collaborative Attacks

In the direct collaborative attack the attacker nodes are already existed in the original network or it joins the network or a node is compromised in the network. The Blackhole and Wormhole attacks are most common example on this category.

A.A.1 Blackhole Attack

In the blackhole attack, the malicious nodes try to disrupt the network routing operation by promoting itself as the shortest path for the destination node. As illustrated in figure 2(a), if node "S" wants to send data packets to Node "D"; for that it first needed a proper route information hence it first broadcast the RREQ (Route Request) to the neighboring nodes. Let the network already consist two collaborative blackhole nodes "B1" and "B2"then they will also receive RREQ from source node. As the property the blackhole these malicious nodes will immediately send the RREP to advertise themselves as the shortest path to destination node "D". Hence when the node "S" receive this RREP it starts transmitting data packets through "B1" and "B2". However because the nodes "B1" and "B2" are working as collaborative backholes, either the "B1" can drop them or it can forward them to "B2"where it can be drop.This results in limited no data packet reception at destination node "D".

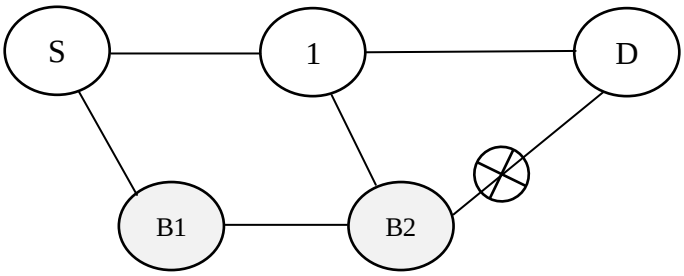

Figure 2(a): Illustration of blackhole attack.

The above scenario show a simple collaborative attack, however more complex collaborative formation between the attacking nodes can be seen for example if node "S" tries to verify the route through "B1" exists using FRQ (further request) [4] through a route not involving "B1" (like S-1-B2). Since the node "B2" is working with in collaboration with "B1" it will verify it with FRP (further reply) that yes route exists [6][4].

A.A.2 Consecutive Collaborative Attack

One more scenario of collaborative attack is presented in figure 2(b) where the attacker align themselves as consecutive node in a route and the first node in the route sends false acknowledgements to previous node that the next node is working normally which is actually not.

IJARCCE

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

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 10, October 2017

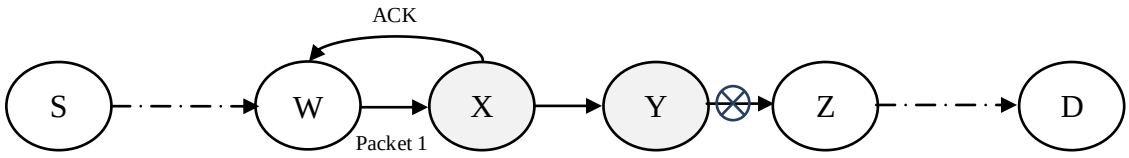

Figure 2(b): Illustration of consecutive collaborative attack

A.A.3 Wormhole Attack

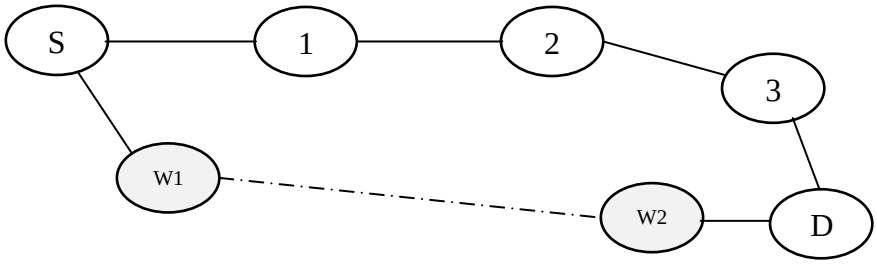

Figure 2(c): Illustration of wormhole attack

The wormhole attack is always required collaborative nodes hence it cannot exist without it.In this kind of attack the two collaborative malicious nodes form a link between them and tunnel data packets back and forth through that link even if the packets not addressed to them. The wormhole attack as illustrated in Figure 2(c), two malicious colluding nodes "W1" and "W2" tunnel data packets to each other to using a separate linkto analyze and tamper the network [4].

B. Indirect Collaborative Attacks

In this type of attack non-existent nodes are created by generating fake identities in order to mislead the other nodes to redirect data packets through malicious node. This type of attack classified as indirect because attacker nodes are not already existing in the original network but where created along the line of their attack. Sybil attack is an example of this kind of collaborative attack. In the Sybil attack malicious node can generate any number of additional fake identities for itself while actually there is only one physical node exist.

IV. PROPOSED ALGORITHM

Considering the attacker has the property to attract the network traffic and drop it. The proposed algorithm utilizes this behavior for detecting the avoiding the paths through such nodes.

Step 1: Let the route [S →1 →A1→A2→7→ D]from node S to Dalready exists which contains theattackers"A1"and"A2",we are considering here that both of attackers "A1" and "A2" can behave independently or collaboratively to drop the data packets.

Step 2: from the figure 3, it is clear that whenever a node transmit a packet the nodes around it (within its transitions range) can also receive the same transmission and so the transmitted packet, irrespective to the fact that the packet may not be intended for them.

Step 3: For every node in the route it is must to forward the each and every data packet it receives for forwarding until the destination reached. Suppose that a node"3" receives a transmission from node "1"then it should also receive the retransmission of the same packet forward by the node "A1" within certain time limits.However if it fails to hear; itmay assume that the node "A1" is misbehaving and dropping, although this assumption may not be true always,considering the fact that the node "A1" can exist in such a position where its transmission cannot reach to node "3".

Step 4: Hence whenever a node heara forwarded data packet transmission by surrounding node it considers the node as a non-malicious and it increases the local trust L_T value for that node. Hereby it is considered that the every node maintains a trust value table for every node it encountered. The nodes also share these trust values with each other's, to making it a collaborative approach. Each node then combines their local trust values with the shared values.

Step 5: The L_T value discussed in step 4 value is used by node not only in route selection procedure but also wheneverit receives aRREQ or RREP to isolate the malicious nodes by estimating thereputation of the node which originated these packets

IJARCCE

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

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 10, October 2017

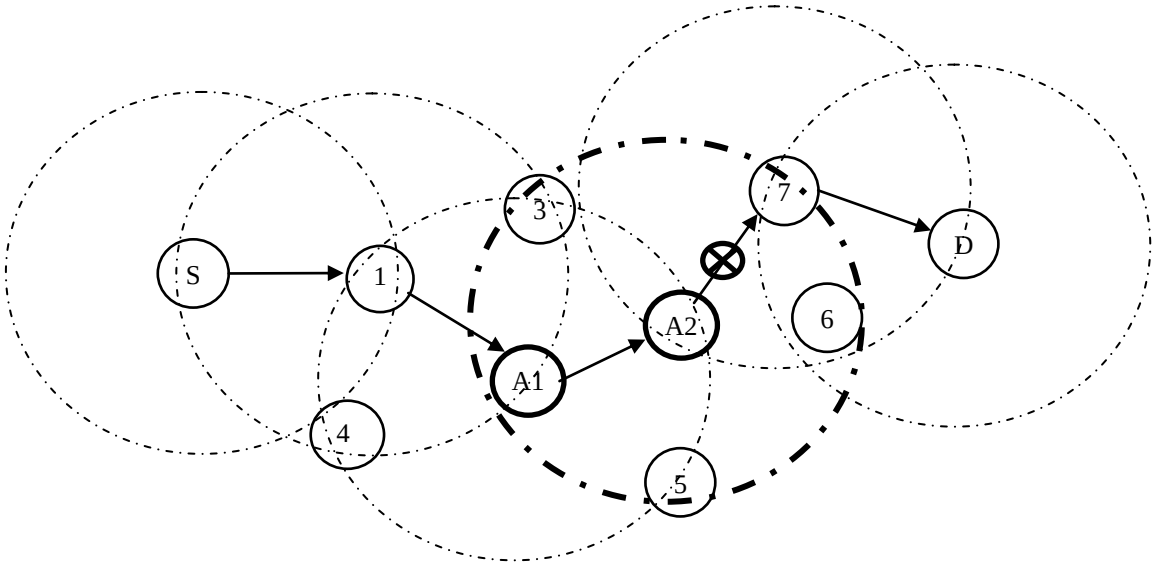

Figure 3: Illustration of proposed algorithm

The algorithm used for the calculation of the node reputation is as follows:
Let L_T be the collaborative trust table of any node which contains trust values for the n different nodes. Let the trust value of the i^{th} node beL_T^i, and the maximum and minimum trust value in the table L_T be L_T^{max} and L_T^{min} respectively. Let the average number of DATA and RREQ packets be P_{DATA} andP_{RREQ} respectively.

Now if at any instant any node receives a RREQ or RREP from the node m. Then first it calculates the reputation of the node m as follows:

$$\text{reputation}_m = \left(\frac{L_T^{max} - L_T^m}{L_T^{max} - L_T^{min}}\right) * \left(\frac{P_{DATA}}{P_{RREQ}}\right)$$

This reputation value is used for the node to decide whether it should forward it or drop it. So if the reputation value of the node is higher than a threshold it should accept it as normal node otherwise it may be considered as malicious.

$$\text{node behaviour} = \begin{cases} \text{normal}, & \text{if reputation}_m > \text{threshold} \\ \text{malicious}, & \text{otherwise} \end{cases}$$

However the above equation may lead to a deadlock if a node fails to transmit a packet because of genuine reasons, hence a much better approach is to give some opportunity to such node by adding a probability of sending even if the node reputation is below threshold.

$$\text{node behaviour} = \begin{cases} \text{normal} & \text{if reputation}_m > \text{threshold} \\ \text{suspicious} & \text{elseif Random} > \text{reputation}_m \\ \text{malicious} & \text{otherwise} \end{cases}$$

In above case even the node having reputation below threshold can get the change considering its behavior suspicious not as malicious.

V. SIMULATION RESULTS

To evaluate the performance of the proposed algorithm, it is simulated using the network simulator environment NS2 for different percentage of malicious nodes. Finally the outcomes of the simulation such as Packet delivery Ration, Throughput and End to End delay are measured to evaluate and compare its performance.

TABLE I SHOWING THE VALUES OF DIFFERENT EVALUATION MEASURES WHEN NETWORK IS UNDER ATTACK AND NO IDS TECHNIQUE IS USED

Network Condition	**Measured Parameters**		
	Throughput	**Delivery Ratio**	**End to End Delay**
Normal	220	0.90	2.45

DOI10.17148/IJARCCE.2017.61015

IJARCCE

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

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 10, October 2017

Attacked (5%)	200	0.79	1.49
Attacked (10%)	190	0.78	1.72
Attacked (15%)	183	0.72	1.78
Attacked (20%)	168	0.65	2.1
Attacked (25%)	150	0.58	2.73
Attacked (30%)	132	0.52	3.91

TABLE III SHOWING THE VALUES OF DIFFERENT EVALUATION MEASURES WHEN NETWORK IS UNDER ATTACK AND A3ACK TECHNIQUE IS USED

Network Condition	**Measured Parameters**		
	Throughput	**Delivery Ratio**	**End to End Delay**
Normal	220	0.90	2.45
Attacked (5%)	210	0.83	1.62
Attacked (10%)	205	0.8	1.69
Attacked (15%)	191	0.78	1.85
Attacked (20%)	163	0.71	1.94
Attacked (25%)	150	0.66	2.31
Attacked (30%)	148	0.59	2.88

TABLE IIIII SHOWING THE VALUES OF DIFFERENT EVALUATION MEASURES WHEN NETWORK IS UNDER ATTACK AND PROPOSED TECHNIQUE IS USED

Network Condition	**Measured Parameters**		
	Throughput	**Delivery Ratio**	**End to End Delay**
Normal	220	0.90	2.45
Attacked (5%)	0.89	1.67	4.27
Attacked (10%)	0.84	1.81	4.22
Attacked (15%)	0.82	1.94	4.98
Attacked (20%)	0.81	2.03	5.1
Attacked (25%)	0.72	2.55	4.8
Attacked (30%)	0.68	3.18	3.5

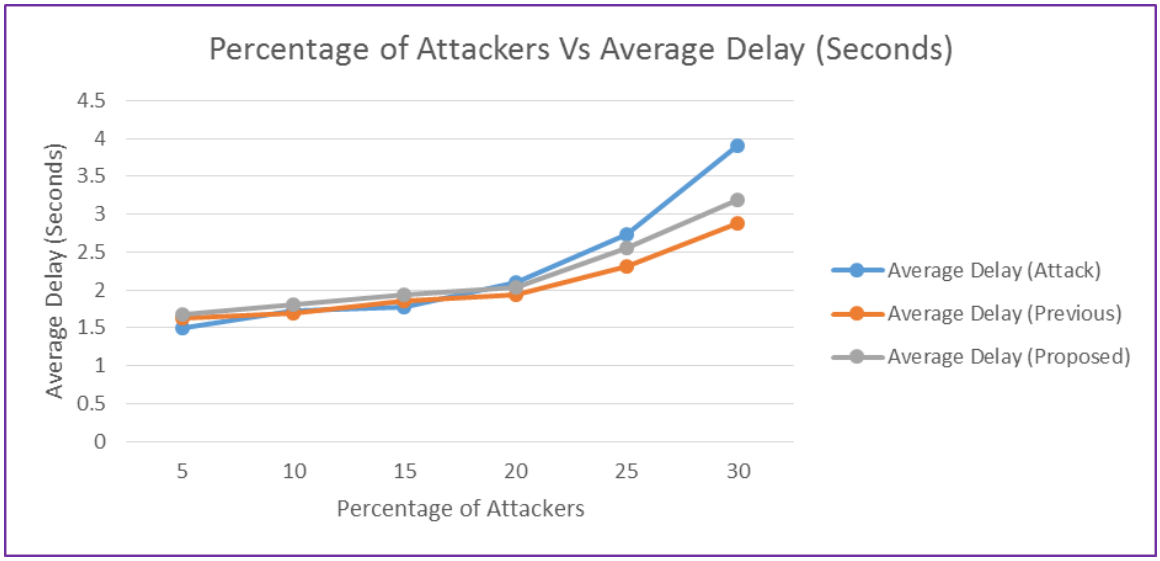

Figure 4(a): Showing impact of Attackers Percentage on Average Delay.

DOI10.17148/IJARCCE.2017.61015

IJARCCE

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

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 10, October 2017

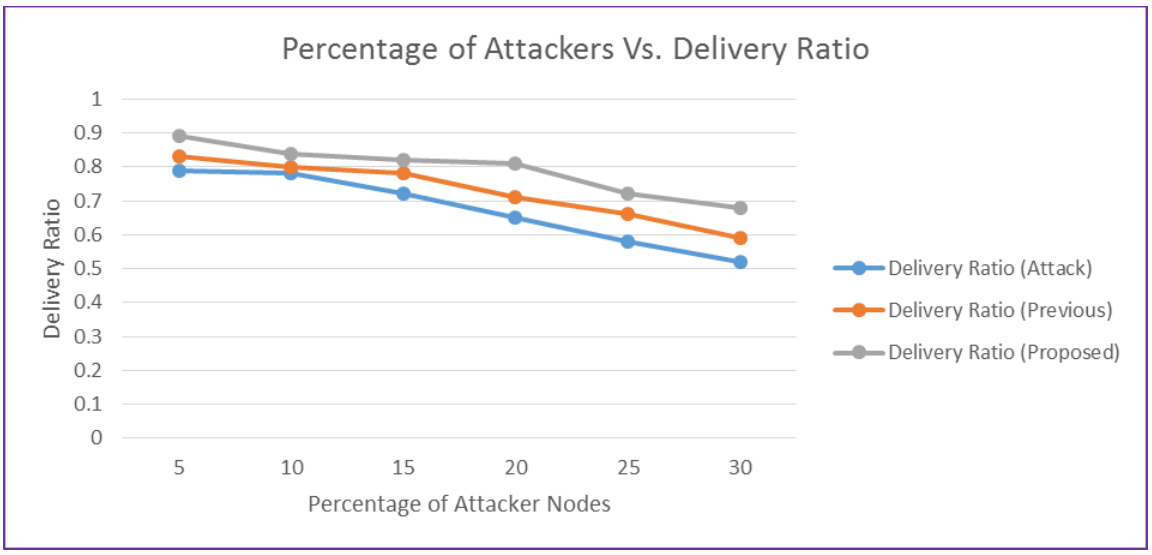

Figure 4(b): Showing impact of Attackers Percentage on Delivery Ratio.

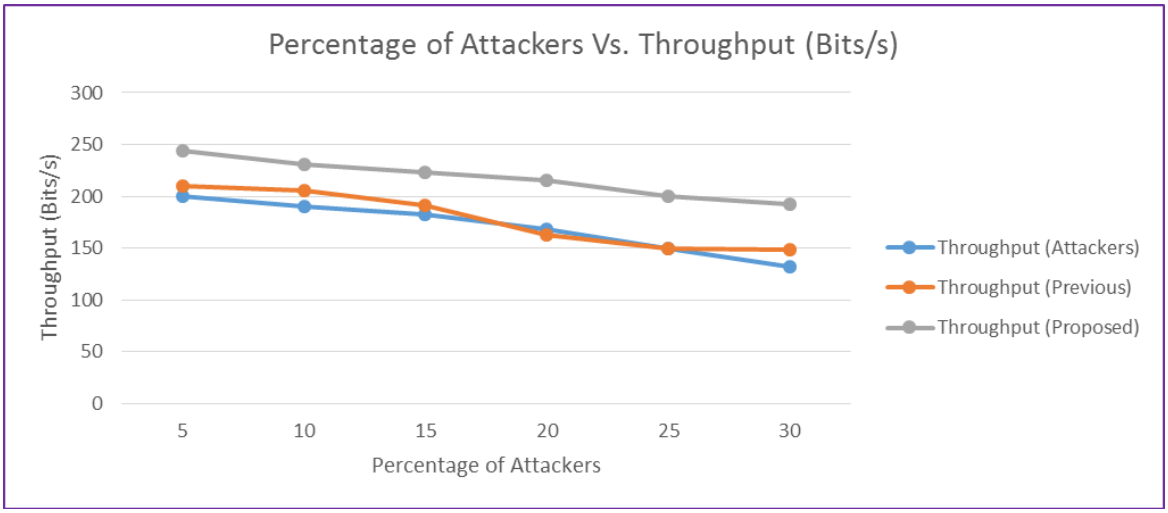

Figure 4(c): Showing impact of Attackers Percentage on Throughput.

VI. CONCLUSION AND FUTURE WORK

In this paper, An Adaptive and Collaborative Enhanced Trust Based Intrusion Detection System is presented and which not only works with non-collaborative packet dropping attacks but also works with different types of collaborative packet dropping attacks. The technique has many advantage such as it can work with different routing protocols such DSR, AODV etc. also it can be integrated with minimal modification in the protocols (only to establish a method for exchanging the trust table).As the simulation result shows it works under the node mobility condition quite well and gives the much better performance than the previous technique. However there is some consideration that can be addressed in the future such as developing the secure and efficient way for exchanging of trust table between the nodes.

ACKNOWLEDGMENT

I would like to acknowledge my Principal at College Samrat Ashok Technology Institute (SATI), vidisha, India and the staff of college and my friends for supporting and motivating me for my research work. I would like to thank my family members for their support.

REFERENCES

[1] AbdulsalamBasabaa, TarekSheltami and ElhadiShakshuki "Implementation of A3ACKs intrusion detection system under various mobility speeds", 5th International Conference on Ambient Systems, Networks and Technologies (ANT-2014).

[2] Al-Roubaiey, T. Sheltami, A. Mahmoud, E. Shakshuki, H. Mouftah "AACK: Adaptive Acknowledgment Intrusion Detection for MANET with Node Detection Enhancement", 2010 24th IEEE International Conference on Advanced Information Networking and Applications.
[3] KashyapBalakrishnan, Jing Deng, Pramod K. Varshney "TWOACK: Preventing Selfishness in Mobile Ad Hoc Networks, Wireless Communications and Networking Conference, 2005 IEEE.
[4] Cong Hoan Vu, AdeyinkaSoneye "An Analysis of Collaborative Attacks on Mobile Ad hoc Networks", Master Thesis Computer Science Thesis no: MCS-2009:4 June 2009
[5] D. Keerthi, Mr. CH. Samson "A Secure Intrusion Detection System for MANETS in Receiver Collisions", International Journal for Research in Applied Science and Engineering Technology (IJRASET)Vol. 2 Issue IX, September 2014
[6] LathaTamilselvan, Dr. V Sankaranarayanan "Prevention of Co-operative Black Hole Attack in MANET", JOURNAL OF NETWORKS, VOL. 3, NO. 5, MAY 2008.
[7] A.Janani, A.Sivasubramanian "Survey of Packet Dropping Attack in Manet", Indian Journal of Computer Science and Engineering (IJCSE)Vol. 5 No.1 Feb-Mar 2014.
[8] D. Helen, D. Arivazhagan"Applications, Advantages and Challenges of Ad Hoc Networks" Journal of Academia and Industrial Research (JAIR) Volume 2, Issue 8 January 2014.
[9] SureyyaMutlu, GurayYilmaz"A Distributed Cooperative Trust Based Intrusion Detection Framework for MANETs," ICNS 2011: The Seventh International Conference on Networking and Services.
[10] Syed Muhammad Sajjad, SafdarHussainBouk, Muhammad Yousaf "Neighbour Node Trust Based Intrusion Detection System for WSN", 6th International Conference on Emerging Ubiquitous Systems and Pervasive Networks,EUSPN-2015.

BIOGRAPHIES

Pooja Malviya M.Tech Scholar in Information Technology and Engineering at Samrat Ashok Technology Institute (SATI), vidisha, India. She has done B.E. in CSE from shri Dadaji Institute of Technology and Science, Khandwa, India. Her area of research is in Algorithms, Mobile Ad-Hoc Network (MANET).

Vivek Sharma An Assistant Professor in Information Technology and Engineering Department at Samrat Ashok Technology Institute (SATI), vidisha, India. He has completed M.Tech in CSE from Samrat Ashok Technological Institute. His main research interests includes Web Application Security & Network Security.