IJETST- Volume||01||Issue||08||Pages 1293-1301||October||ISSN 2348-9480 2014

Open access Journal International Journal of Emerging Trends in Science and Technology

Remote Adaptive Sensing Based Malicious Node Detection and Security in MANET'S

Authors
Vittal S[1], B.Nagalakshmi[2], Venkatesh .D[3]
[1]M.Tech Student, Dept. of CSE, GIT, Gooty, Anantapur, India
Email: *vittal.dhl@gmail.com*
[2]Asst. Prof, Dept. of CSE, GIT, Gooty, Anantapur, India
Email*: nagalakshmi623@gmail.com*
[3]Prof. & Dean, Dept. of CSE, GIT, Gooty, Anantapur, India
Email: *deancseit@gmail.com*

Abstract

The technology of networks is shifted to non-wired networks which are widely accepted in the recent years. Addition of components to the wireless network a varied uses in many areas and one such use is found in mobile ad hoc network (MANET).All the hosts in the network have a dual functionality of both sending and receiving messages within Transmission range. Any failure of single node in the network will not harm the network functionality, has the capacity of rebuilding itself, and therefore its finds its use in defense and many other applications. but still there exists threat of location of nodes is not centralized .Any attack of a virus or any other threats to the network which can be self-replicating is called as an intrusion and such intrusion must be detected and also prevented .This is required in case of MANETS'S are use in various commercial applications. This intrusion detection system is named as RAMND for MANET'S with which higher security can be achieved.

Keywords— *Elliptic Curve Cryptography, Mobile Ad hoc Network, Remote Adaptive Sensing Based Malicious Node Detection and Security in MANET'S*

INTRODUCTION

Due to their natural quality and measurability, wireless networks are continually most well-liked since the primary day of their invention. Due to the improved technology and reduced prices, wireless networks have gained way much more preferences over wired networks in the recent years. Mobile Ad hoc Network (MANET) can be an assortment of mobile nodes equipped with a non-wired receiver and a transmitter that communicate with each other via two-way wireless links either directly or indirectly. Industrial remote access and management via wireless networks have become additional standard of late. One in all the main use of wireless networks is its ability to permit digital communication between totally different parties and still maintain their quality. However, this communication is restricted to the range of transmitters. This implies that two nodes cannot communicate with one another once the gap between the two nodes is on the far side the communications range of their own. MANET solves this drawback by permitting intermediate parties to relay knowledge transmissions. This result is dividing MANET into two types of networks, they are multihop and single-hop in an exceedingly single-hop network, all nodes among a similar radio range communicate directly with one another. In exceedingly multihop network nodes admit totally different intermediate nodes to transmit if the destination node is out of their radio range. In contrary to the traditional wireless network MANET contains a sub-urbanized network infrastructure.

MANET doesn’t need a set infrastructure; so, all nodes are unengaged to move randomly [8], [9], [10]. MANET is capable of making a self-configuring and self-maintaining network while not the assistance of a centralized infrastructure, that is usually impossible in mission critical applications like military conflict or emergency recovery. Marginal configuration in a quick preparation build MANET ready to use in emergency circumstances where wherever infrastructure is unfeasible to place in eventualities like natural disasters, military conflicts and medical emergency things. Owing to these distinctive characteristics, MANET is becoming essential and wide enforced within the trade. However, considering the very fact that MANET is well-liked among important mission applications, network security is of significant importance. The open medium and remote distribution of MANET build it at risk of numerous kinds of attacks.

As a result of the nodes lack of physical protection, malicious attackers will simply capture and compromise nodes to attain attacks. Specially, considering the actual fact that almost all routing protocols in MANETs assume that each node within the network behaves tending to cooperation to with alternative nodes and presumptively not malicious attackers will simply compromise MANETs by inserting malicious or non-cooperative nodes into the network. Moreover MANET’s distributed design and dynamic topology, a standard centralized observance technique is not any longer possible in MANETs. Under these conditions, developing an intrusion-detection system (IDS) specially designed for MANETs becomes crucial.

EXISTING SYSTEM

As mentioned before, owing to the limitations of most MANET routing protocols, nodes in MANETs assume that alternative nodes continuously collaborate with one another to relay knowledge. This assumption leaves the attackers with the opportunities to attain important impact on the network with only one or two compromised nodes. To deal with this downside, associate IDS ought to be more to boost the protection level of MANETs. If MANET will notice the attackers as before long as they enter the network, we are going to be ready to fully eliminate the potential damages caused by compromised nodes at the primary time. IDSs sometimes act because the second layer in MANETs, and that they square measure an excellent complement to existing proactive approaches [12], [13] .

1) Watchdog: Marti et al. [1] proposed a Watchdog achieves the maximum output in the network even if a malicious node exists, so this scheme is made up of two entities namely watchdog and pathrater. Watchdog is associate IDS for MANETs. It's in charge of detection malicious node misbehavior within the network. Watchdog detects malicious misbehavior by promiscuously taking note to its next hop's transmission. If a Watchdog node overhears that its next node fails to forward the packet among an exact quantity of your time, it'll increase its failure counter. Whenever a node's failure counter exceeds a predefined threshold; the Watchdog node reports it as misbehaving. Throughout this case, the Pathrater cooperates with the routing protocols to avoid the re moveable nodes in future transmission. Several following analysis studies and implementations have proved that the Watchdog theme is economical Moreover, compared to another schemes, Watchdog is capable of detection malicious nodes instead of links. These benefits have created the Watchdog plan of action a well-liked alternative within the field. Several MANET IDSs area unit either supported or developed as associate improvement to the Watchdog plan of action [2], [3], [4], [5]. Yet, as discerned by Marti et al [1]. , the Watchdog plan of action fails to discover malicious misbehaviors with the presence of the following:1) ambiguouscollisions;2)receiver collisions; 3)false misbehavior report;4)limited transmission power;5)collusion; and 6) partial dropping.

2) TWOACK: The six Limitations of the Watchdog Scheme, TWOACK planned by Liu et al [6]. TWOACK is neither associate degree improvement nor a Watchdog-based scheme. Going to resolve the receiver collision and Limited transmission power problems of Watchdog, TWOACK detects

misbehaving nodes by acknowledging each information packet transmitted over each three consecutive nodes on the trail from the supply to the destination. Upon retrieval of a packet, every node on the route is needed to remit associate degree acknowledgment packet to the node that two hops far from it down the route. The operating method of TWOACK is shown in Fig. 1: Node a primary forwards Packet 1 to node B, and then, node B forwards Packet one to node C. once node C receives Packet one, because it is 2 hops far from node A, node C is obligated to get a TWOACK packet, that contains reverse route from node A to node C, and sends it back to node A. This TWOACK packet isn't received in an exceedingly predefined period, each nodes B and C are malicious.

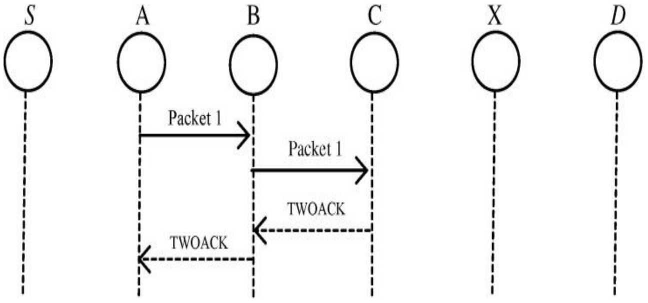

Fig. 1. TWOACK scheme

The TWOACK scheme with successfully solves the receiver collision and Limited transmission power issues shown by Watchdog. However, the acknowledgment method needed in each packet transmission method else a big quantity of unwanted network overhead. Because of the restricted battery power nature of MANETs, such redundant transmission method will simply degrade the life of the complete network.

3) AACK: To support TWOACK, Sheltami et al [5]. Proposed a new scheme known as AACK, AACK is associate degree acknowledgment-based network layer scheme which may be thought-about as a mixture of a scheme known as TACK and an end-to-end acknowledgment scheme known as Acknowledge (ACK). Compared to TWOACK, AACK has considerably reduced network overhead whereas still capable of maintaining or maybe surpassing identical network throughput.

In MANET's, there exists several kinds of disadvantages as discussed above, but in order to overrule those entities, we have proposed a scheme in which malicious nodes can be easily identified and one can switch from malicious node to other nodes by using remote adaptive sensing mechanism, This consists of four distinguished parts. This helps in routing The packets to non-malicious nodes, in fact, multiple existing acknowledgement schemes are not so effective including TWOACK and AACK which do not address the problem of negative acknowledgment there by not assuring packet delivery, so to overcome this, we are using a elliptic curve cryptography in our proposed system. Hence it's called as Remote Adaptive Sensing of malicious node with security in MANET's.

PROPOSED SYSTEM

Our proposed approach RAMND is designed to tackle four of six weaknesses of watch dog scheme, namely, false misbehavior, limited transmission power, ambiguous collision and receiver collision.

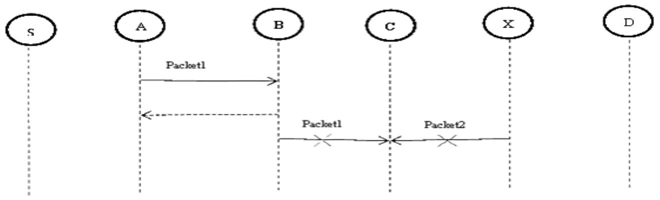

Fig. 2. Receiver collisions

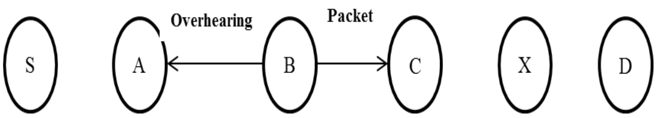

Fig. 3. Limited transmission power

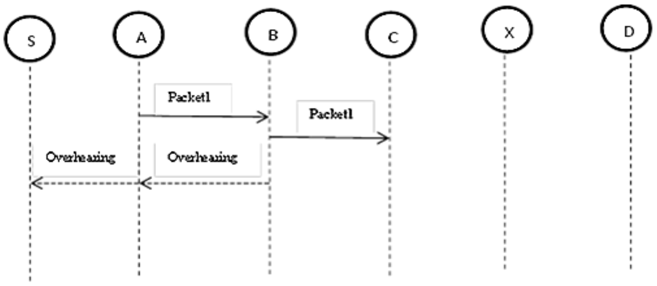

Fig. 4. False misbehavior report

In a typical example of receiver collisions, shown in Fig. 2, node A transmits Packet 1 to node B, node A eavesdrops the packet send from node B to node C; at the same time, node X sends Packet 2 to node C. In such case, node A eavesdrops the packet that node B has with success forwarded Packet 1 to node C however did not observe that node C failed to receive this packet as a result of a packet collision between one and two at node C.

In the case of limited transmission power, in order to pre-serve its own battery resources, node B advisedly limits its transmission power so it's robust enough to be overheard by node A however not robust enough to be received by node C, as shown in Fig. 3.

For false misbehavior report, though node A with success overheard that node B forwarded Packet one to node C, node A complaining node B as a malicious, as shown in Fig. 4. As a effect of the wireless medium and remote distribution of unique MANETs, attackers will attack one or two nodes to understand false misbehavior report.

As specified in above sections, two weaknesses namely, lesser transmission power, unexpected collisions at the receiver are resolved by using TWOACK and AACK. However, each of them is vulnerable to the false misbehavior attack. During this analysis work, our goal is to propose an IDS specially designed for MANETs, that solves not solely receiver collision and limited transmission power however additionally the false misbehavior downside.

RAMND consist of four parts namely ACK, secure-ACK, Misbehavior Report authentication (MRA) and ACA.

1. ACK:

ACK is considered to be an acknowledgement scheme between any two peers which specifies hybrid scheme and increases the size of backend network.

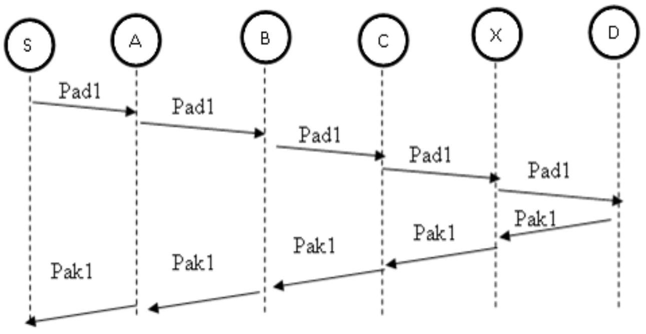

Fig. 5. ACK scheme

In ACK mode, when node S acknowledges by sending packet pad1 to node D, node D will send acknowledgement packet pad1, if all the nodes between S and D are non malicious, on the same route however in a very reverse order. Among a predefined amount of time, on reception of pak1 by node S it is said to be a successful transmission between node S and node D. In case of unsuccessful transmission node S migrate to S-ACK state by transmitting S-ACK packet to discover the misbehaving nodes within the route.

2. S-ACK :

The S-ACK is a better option over TWOACK scheme proposed by Liu *et al.* [6]. The idea is to use any three continuous nodes in a bunch to find misbehaving nodes. For every third node in a set of three nodes will send S-ACK acknowledgement to primary node. The advantage of using S-ACK mode is to find faulty nodes whenever a collision occur or there is a limited transmission power.

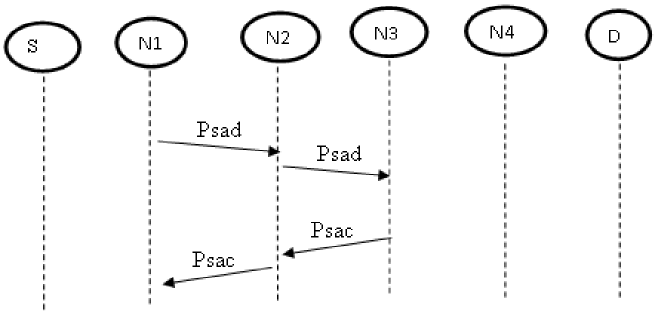

Fig. 6. ACK scheme

The three consecutive nodes (i.e., N1, N2, and N3) add a bunch to find misbehaving nodes within the network. Node N1 initial sends out S-ACK information packet Psad1 to node N2. Then, node N2 forwards this packet to node N3. Once node N3 receives Psad1, because it is that the third node during this three-node cluster, node N3 is required to transmit back an S-ACK acknowledgment packet Psack1 to node N2. Node N2 forwards Psack1 back to node N1. If node N1 doesn't receive this acknowledgment packet at intervals a predefined time period, each node N2 and N3 are rumored as malicious. Moreover, a misbehavior report are generated by node N1 and sent to the source node S. Nevertheless, unlike the TWOACK scheme, wherever the source node in real time trusts the misbehavior report, RAMND needs the source node to change to MRA mode and ensure this misbehavior report. This is often an important step to find false misbehavior report in our proposed scheme

3. MRA:

The MRA scheme is intended to give solution to the weakness of Watchdog because it fails to find misbehaving nodes with the presence of false misbehavior report. The false misbehavior reports are often generated by malicious attackers to incorrectly report innocent nodes as malicious. This attack is often fatal to the whole network once the attackers break down adequate nodes and therefore results in split of a network. The basic of MRA scheme is to verify whether the missing packets through an alternative route. To start the MRA mode, the source node first searches its local knowledge domain and seeks for another route to the destination node. If there's no different exists, the source node starts a DSR routing request to seek out another route. Because of the character of MANETs, it's common to seek out multiple routes between two nodes [7].

By including another route to the destination node, we have a tendency to circumvent the misbehavior communicator node. Once the destination node receives an MRA packet, it Searches its local knowledge domain and compares if the reported packet was received. If it's already received, then it's safe to conclude that this is often a false misbehavior report and whoever generated this report is marked as malicious. Otherwise, the misbehavior report is trustworthy and accepted. By the adoption of MRA scheme, RAMND is capable of detecting malicious nodes despite the existence of false misbehavior report.

4.ACA:

The ACA scheme is designed to resolve the weakness of Watchdog once it fails to handle ambiguous collision. Token bucket is traffic filter where token bucket Size T and the token rate U are the two parameters. The Token Bucket holds the Tokens. Tokens are generated for every clock cycle in host system. The arriving of packet with size can be sum of tokens size in bucket, if not the arriving packet will be discarded. To transmit a packet, host must capture and use the token. The size of transmitting packet must be of size of used token. The outgoing packet rate must be same as token rate U. Once the bucket is full, newly generating tokens are also discarded. So by using the Token Bucket Algorithm, the occurrence of congestion will be avoided in-turn avoiding the collision.

Elliptic Curves Cryptography:

Key exchange using elliptic curve can be done in the following manner. First pick a large integer q, which is either a prime number P or an integer of the form 2^mAnd elliptic curve parameters a and b.

$$Y^2 \bmod p=(x^3+ax+b) \bmod p$$

OR

$$y^2+xy=x^3+ax^2+b$$

This defines the elliptic group of points $E_q(a,b)$ A base point G=(x,y) in Ep(a,b) whose order is very large value n.

User A key generation:

Select private n_A

$n_A < n$

Calculate public P_A

$P_{A=}n_{A*G}$

User B key generation:

Select private n_B

$n_A < n$

Calculate public P_B

$P_{B=}n_{B*G}$

Generating of secrete key by user A

$K=n_B*p_B$

Generating of secrete key by user B

$$K=n_B*p_A$$

ECC Key exchange

Elliptic curve Encryption and decryption. In this system is to encode the plain text message m to be sent as an x-y point P_m.

It is the point P_m that will be encrypted a cipher text and subsequently decrypted.

To encrypt and send a message Pm to B, A chooses a random positive integer K and produces the cipher text Cm. consisting of the pair of points.

$$C_m=\{K_G, P_m+KP_B\}$$

To decrypt the cipher text , B multiplies the first point in the pair by B's secrete key and subtracts the result from the second point.

$$P_m+KP_B - n_B(KG)= P_m+K(n_BG) - n_B(K_G)=P_m$$

PERFORMANCE EVALUATION

It is necessary to discuss the concepts of simulation and its usage as well as measure its effectiveness by using simulation and having a simultaneous study of its output in contrast with watchdog, TWOACK , RAMND scheme.

For analyzing the efficiency of the RAMND under various kinds of threats, we discuss a model to understand the kinds of threats.

Scenario 1: In this scenario, we simulated a basic packet-dropping attack. Malicious nodes discards all the kinds of packets upon reception, so we need to study the efficiency such IDS's in comparison with drawbacks of IDS's namely receiver collusion and limited transmission power.

Scenario 2: This scenario is designed to test IDSs' performances against false misbehavior report. In this case, malicious nodes always drop the packets that they receive and send back a false misbehavior report whenever it is possible.

Scenario 3: This scenario is useful in watching IDS's effectiveness against attackers which are quite intelligent to after the ACK packets and send affirmative results. We continue to adopt the following two performance metrics [11].

1) Packet delivery ratio (PDR): PDR status the proportion of packets that are to be transmitted by the source and to be delivered to the receiver.

2) Routing overhead (RO): RO gives the quality of packets that are routed into the network Route Request (RREQ), Route Reply (RREP), Route Error (RERR). Upon receiving this RREQ message, every adjacent neighbor adds its own addresses to the received message and later sends this message to all its neighbors. If a failing node is detected, that usually indicates a broken link in flat routing protocols like DSR, and a message of RERR, is transmitted the source node .the receiver or destination node generates an RREP message and send the message to the source node via the reveres route within the RREQ message Simulation Results—Scenario 1: In scenario 1, malicious nodes discards the packets that pass through it. Fig. 7. As per results of simulation results that are based on PDR.

Scenario 1: Packet Delivery Ratio

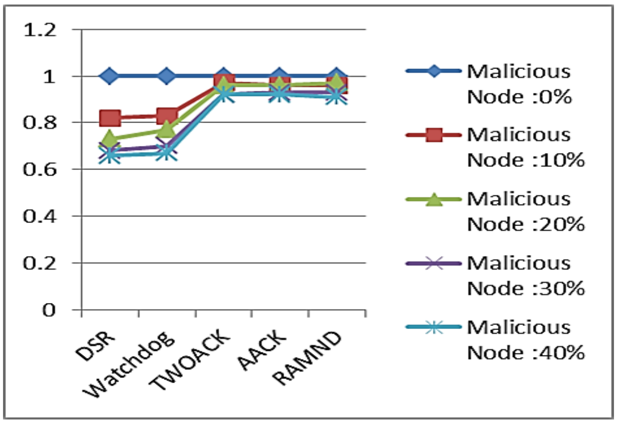

Fig.7. Simulation results for scenario 1-PDR

In contrast to watchdog scheme, IDS's scheme that provide acknowledgement has a better performance. Our proposed scheme RAMND surpassed Watchdog's performance by 21%

When there are 20% of malicious nodes in the network. As per the results of simulation, two schemes namely TWOACK, AACK are detecting malicious nodes even in the case of collisions at the receiver and limited transmission power . But when the percentage of malicious nodes is 40% , RAMND performance is reduced when compared to TWOACK and AACK.

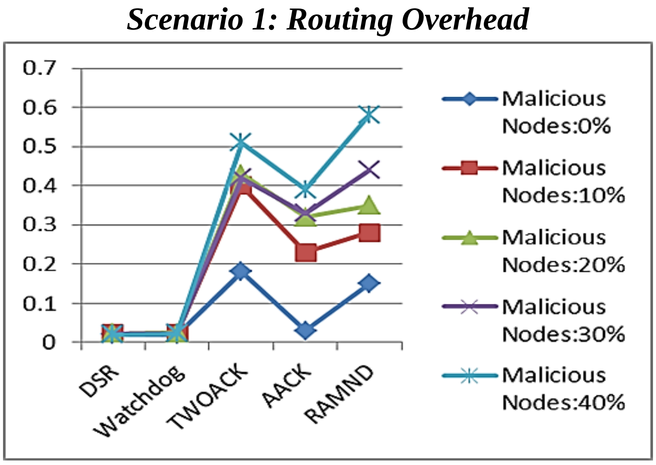

Fig. 8. Simulation results for scenario 1—RO

The simulation results of RO in scenario 1 shown in Fig. 8. We have a tendency to observe that DSR and Watchdog scheme come through the most effective performance, as they are doing not need acknowledgment scheme to observe misbehaviors. For the remainder of the IDSs, AACK has least overhead. This is often for the most part thanks to its hybrid design that considerably reduces network overhead.

2) Simulation Results—Scenario 2: within the second scenario, we have a tendency to set all malicious nodes to send out false misbehavior report back to the source node whenever it's potential. This scenario setting is meant to check the IDS's performance under the false wrongful conduct report. Fig. 9 shows the achieved simulation results supported PDR. Once malicious nodes re 10% percent, RAMND performs a 2% than AACK and TWOACK. Once the malicious nodes are 20% and 30%, RAMND outperforms all the opposite schemes and maintains the PDR To 90%. We have a tendency to believe that the introduction of MRA scheme in the main contributes to the current performance. RAMND is that the solely scheme that's capable of detecting false misbehavior report.

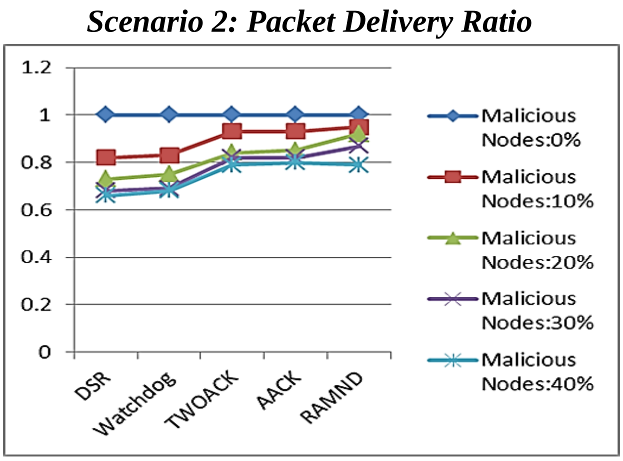

Fig. 9. Simulation results for scenario 2—PDR

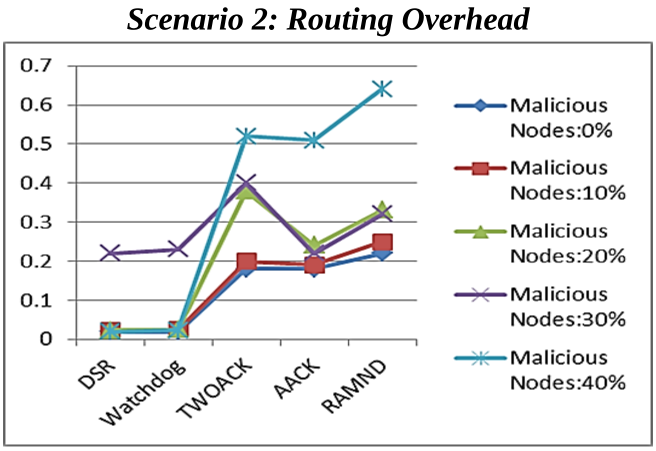

Fig. 10. Simulation results for scenario 2—RO

3) Simulation Results—Scenario 3: In scenario 3, we have a tendency to provide the malicious nodes have the advantages of forging the packets by which they discard all the packets that have been received and sends out forged packets for which acknowledgement here already been received. This is often a standard technique for attackers to degrade network performance whereas still maintaining its name.

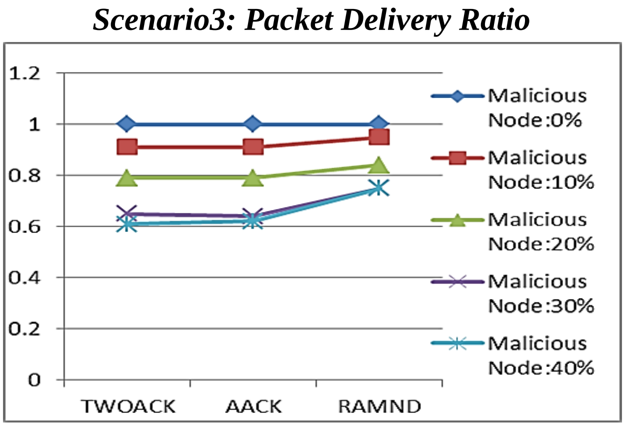

Fig. 11. Simulation results for scenario 3—PDR

Scenario 3: Routing Overhead

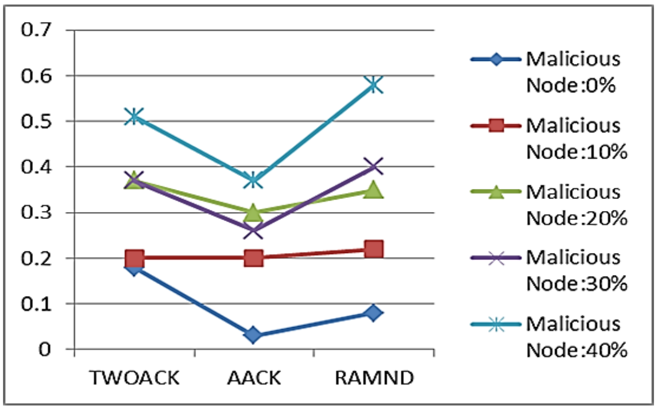

Fig. 12. Simulation results for scenario 3—RO

The PDR performance comparison in situation 3 is shown in Fig. 11. We are able to observe that our proposed scheme RAMND outperforms TWOACK and AACK all tests. We can't come to a conclusion that RAMND is the exclusive option available that can identify duplicate packets.

CONCLUSION AND FUTURE WORK

Packet-dropping attack has continuously been a serious threat to the protection in MANETs. In this paper we have projected unique IDS named RAMND protocol is the only one meant for MANETS and later was able to differentiate in several methodologies in simulations. The results incontestable positive performances against Watchdog, TWOACK, and AACK within the examples of limited transmission power, ambiguous collision, false misbehavior report and receiver collision.

Furthermore, in an effort to stop the attackers from initiating cast acknowledgment attacks, we tend to extend our analysis to include ECC in our proposed scheme. Al-though it generates a lot of ROs in some cases, as incontestable in our experiment, it will vastly improve the network's PDR once the attackers are good enough to forge acknowledgment packets.

In future reaming issues of Watchdog, Partial dropping and collusion can be avoided.

REFERENCES

1. Djahel, S. , Nait-abdesselam, F. , Zonghua Zhang " Mitigating Packet Dropping Problem in Mobile Ad Hoc Networks: Proposals and Challenges" Communications Surveys & Tutorials, IEEE , Volume: 13 , Issue: 4,pp 658 - 672 ,2011
2. J.-S. Lee, "A Petri net design of command filters for semiautonomous mobile sensor networks," *IEEE Trans. Ind. Electron.*, vol. 55, no. 4, 1835–1841, Apr. 2008.
3. Badie, A.M. "Responding to intrusions in mobile ad hoc networks"Inf.Syst. Security Manage., Concordia Univ. Coll. of Alberta, Internet Security(World_CIS), 2013 World Congress , pp 30 – 34, 2013
4. A. Patcha and A. Mishra, "Collaborative security architecture for black hole attack prevention in mobile ad hoc networks," in *Proc. Radio Wire-less Conf.*, 2003, pp. 75–78.
5. T. Sheltami, A. Al-Roubaiey, E. Shakshuki, and A. Mahmoud, "Video transmission enhancement in presence of misbehaving nodes in MANETs," *Int. J. Multimedia Syst.*, vol. 15, no. 5, pp. 273–282, Oct. 2009.4
6. Sowmiya Hariharan, Jothi Precia, Suriyakala. C.D, Prayla Shyry "A Novel Approach for Detection of Routes with Misbehaving Nodes in MANETs"ACEEE Int. J. on Network Security, Vol. 02, No. 01, Jan 2011
7. Kok-Poh Ng ; Tsimenidis, C. "Energy-balanced dynamic sorce routing protocol for wireless sensor network" Wireless Sensor (ICWISE), 2013 IEEE Conference, pp 36-41, 2013
8. Bahuguna Renu, Mandoria Hardwari lal, Tayal Pranavi "Routing Protocols in Mobile Ad-Hoc Network: A Review", the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering Volume 115, 2013, pp 52-60
9. Boppana, R.V. , Xu Su "On the Effectiveness of Monitoring for Intrusion Detection in Mobile Ad Hoc Networks"

IEEE Trans. Mobile Comput., vol. 10, issue 8, pp 1162 - 1174 , 2011

10. A. Tabesh and L. G. Frechette, “A low-power stand-alone adaptive circuit for harvesting energy from a piezoelectric micropower generator,” *IEEETrans. Ind. Electron.*, vol. 57, no. 3, pp. 840–849, Mar. 2010.
11. N. Kang, E. Shakshuki, and T. Sheltami, “Detecting forged acknowledgements in MANETs,” in *Proc. IEEE 25th Int. Conf. AINA*, Biopolis, Singapore, Mar. 22–25, 2011, pp. 488–494.
12. R. H. Akbani, S. Patel, and D. C. Jinwala, “DoS attacks in mobile ad hoc networks: A survey,” in *Proc. 2nd Int. Meeting ACCT*, Rohtak, Haryana, India, 2012, pp. 535–541.
13. A. Tabesh and L. G. Frechette, “A low-power stand-alone adaptive circuit for harvesting energy from a piezoelectric micropower generator,” *IEEE Trans. Ind. Electron.*, vol. 57, no. 3, pp. 840–849, Mar. 2010.