EA3ACK - A Secure Intrusion DetectionSystem using FA Logic for MANET

K. Thamizhmaran
Dept. of ECE, GCE Bodinayakkanur
Theni, Tamilnadu, India - 625582

Abstract: *Mobile ad hoc networks (MANETs) do not have a fixed infrastructure. All the nodes in the MANET act as the both receiver and transmitter. Each node directly communicates with the other when they are both within their communication range. Each nodes work as routersand take path in discovery and maintenance of routes to other nodes in the network. MANETnodes square measure distinguished by their restrictedresources like security, energy, bandwidth, processing and storage.Routing in MANET is serious issue as a result of topologyi.e. changeable because of nodes quality. Particularlyenergy economical routing is most vital as a result of allthe nodes square measure battery powered. In this paper,proposed a new secure routing technology called Enhanced Adaptive 3 Acknowledgement (EA3ACK), usingEnhanced Adaptive Acknowledgement (EAACK) with Fuzzy Approach (FA) Logic designed for MANET. In the fuzzy approachis used to detect misbehaving node by giving certificate to only trusted node. The proposed EA3ACK - FA technique is more secure and reliable to increase the network lifetime, packet delivery ratio, throughput and routing overhead with fixed topology size by continuously monitoring the individual nodes in the network. Network simulator (NS2) is used to simulate and analysisthe proposed system.*

Keywords — *MANET; Routing Protocols; Network Security; IDS;EAACK; FA;EA3ACK-FA; PDR; RO;Throughput; Remaining Energy.*

I. INTRODUCTION

MANETs are a group of autonomous wireless mobile nodes that communicate with one another to form a multi-hop wireless radio network. Every node has a wireless interface to communicate with the other radio waves. Personal Computers (PC) and Personal Digital Assistants (PDA) to communicate directly with each other like some examples of nodes in a MANET. Fig. 1 shows a simple MANET with three nodes. MANET does not use any centralized administration. Nodes can able to join / leave the network as they wish. Multiple hop nodes may be needed to move other nodes, because of its transmission range limits of the nodes. Any node who is willing to participate in ad hoc network should forward the packets to other nodes. Ad hoc network handles the problems such as network structure changes and malfunctions of nodes through network reconfiguration. For example, if a node can join the network and causes a link breakage, the affected node could easily give the request for a new route and the packet is communicated through the new route. But this will increase the end-to-end delay (Basagni*et al.* 2004). The MANETs characteristics include, dynamic topologies, limited bandwidth, energy constrained, limitations of the medium, and limited physical security (Gross glauser and Tse 2002, Wu and Dai 2005).Some of the applications of MANET are virtual classrooms, conferencing, emergency services, personal area network, disaster relief operations and military applications.

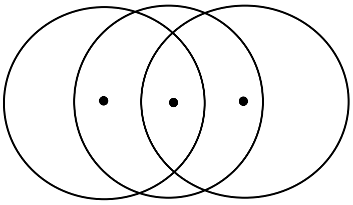

Fig. 1 Simple MANET

Routing deals with finding appropriate paths from source node to destination node, possibly over many intermediate nodes. Classical routing protocols for the fixed wired network is do not adequate for ad hoc networks and perform poorly because of these network's distinct characteristics, like the rapidly changing topology, the broadcast propagation medium. Many routing protocols have been designed for an ad hoc network.Classifications of routing protocols for MANET can be done on routing strategy wise or topology wise. Classification of routing protocol according to routing strategy wise is three parts table driven, on-demand and hybrid. All these protocols behave differently on wireless conditions. For example, mobility of node may cause link breakage, which adversely impact routing and QoS support. Size of the network and routing overhead will have considerable impact on network scalability along inherent characteristics of the ad hoc networks which may be result in unpredictable variations in performance of the entire network (Royer and Toh 1999, RCF 2501 1999). Some issues MANETs are: congestion (when more number of packets send to the network and more number of packets a network can handle), energy efficiency (when retransmitting of packet, increasing time duration of path finding and link breakage), security (when node can join and leave to affect network performance, involve internal external attacks due to air medium), QoS (provide better service to selected network traffic), bandwidth and mobility of node (changing network topology, node move to other network). In next section, some security issues are presented which characterize the MANET security.One of the important issues of MANETs is security for more sensitive applications used in military communications and other critical communications. A MANET can be considered secure if it holds these attributes: confidentiality, integrity, availability, authentication, non-repudiation, and access control (Marti *et al.* 2000, Yang *et al.* 2004).A security attack is any action that compromises the security of information in an unauthorized way. The attacks on the MANETs can be broadly classified into two categories: passive and active attacks.

All routing protocols perform two important functions: (i) Routing function and (ii) Data forwarding function. The routing function involve in path finding and path maintenance, whereas data forwarding function performs forwarding data packets towards the destination via already established route. Routing function is affected in the presence of inactive nodes. It is called malicious nodes which can cause various types of attacks, like packet eavesdropping, active and passive attacks. A malicious node simply drops all packets as shown Buchegger*et al.*2003.Packet drop occurs when one or more packets of data travelling across a network fail to reach their destination, mobility of topology, traffic, environment condition, and link breakage, selfish and malicious attacks.Intrusion Detection System (IDS) is required to detect the malicious attack before it can accomplish any significant damage to the network.IDS are used to detect the malicious nodes and to avoid packet dropping in MANET. It should be cooperative and power efficient and suitable for dynamical change in network structure and limited battery power of the mobile nodes in MANET. It increases Packet Delivery Ratio (PDR), decreases overhead and delay in MANET (Puketza*et al.* 1996, Denning 1987). Watchdog serves as IDS for MANETs and also responsible for removing malicious nodes in the network.

In each node maintains path of the packets which it sent. It contains a unique packet id, address of the next node to which the packet was forwarded, address of the destination node and an expiry time after which a still existing packet in the buffer is considered not forwarded next node. In node rating table, each node maintains rating of adjacent node. The last field of the node rating table is calculated by the ratio of dropped packets and successfully forwarded packets, if this ratio is greater than a given threshold value then this node misbehave value will be 1(means it is considered as a misbehaving node), otherwise it is considered as a genuine node. An expired packet in the pending packet table causes the packet drops counter to increment for the next hop associated with the pending packet table entry. For deciding whether a node is misbehaving or act as a legitimate one, depend on the selection of threshold value. For example if we take a threshold value of 0.5. This means that as long as a misbehaving node is forwarding twice packets as it drops it will not be detected. If we take a lower value of threshold then it will increase the percentages of false positives.The advantage of watchdog is that it is capable of detecting malicious at the forwarding level instead of just on the link level. The disadvantage of watchdog is that it may fail to detect a misbehaving node in the presence of 1) ambiguous collisions 2) receiver collisions 3) limited transmission power 4) false misbehaviour report 5) collusion and 6) partial dropping. Several techniques are available for overcoming the drawbacks of watchdog in MANET.With respect to the six weaknesses of the watchdog scheme, many researchers proposed new approaches to solve these issues such as, acknowledgement, detection graph, numbering, bayesian filtering method, and halt. Acknowledgement is one of the most significant approaches among them.There are various challenges that have to be taken into account when designing a MANET. In MANET the energy of one node is powered by batteries with limited energy. Therefore the minimal energy node can roll as selfish node. The energy of a node is calculated by the energy spent on transmission and the reception of data packets and acknowledgements. MANET attracted by the attackers because its unique features like dynamic topology, variable capacity, open medium, local physical security and energy constrained operation. In military application mobility is a critical factor because mission will start at certain coordinate and will end up at the other coordinate. In the battle field soldiers exchange the message like voice recording, video tapes, images and quality of services to other field unit. Unfortunately the communication can have delay of message, dropped message and delivery of erroneous. To improve the performance the proposed scheme provides trust based data exchange, certificate authority and fuzzy based analyzer to detect the misbehaving node. EAACK, EA3ACK and EA3ACK-FA routing protocols used in military application because the source node maintains the routes as long as need by itself. It is reactive protocols, when a node wishes to start transmission with another node in a network to which it has no route; the topology information is provides by the EAACK, EA3ACK and EA3ACK-FA protocols.

II. Existing System

2–ACK/3-ACK

In 2-ACK mode, the three consecutive nodes (i.e., A, B, C) work in a group to overcome the drawbacks of watchdog scheme in the network. Node A first sends out 2-ACK data packet P1(S) to node B. Then, node B forwards this packet to node C. When node C receives P1(S), as it is the third node in this three-node group, node C is required to send back a 2-ACK acknowledgement packet P1 (A) to node B. Node B forwards this P1 (A) back to node A. If node A does not receive this acknowledgement packet within a predefined time period, both nodes B and C are reported as malicious. This process is shown in Fig. 2. In 3-ACK mode, the four consecutive nodes (i.e., A, B, C, and X) work in a group to overcome the drawbacks of watchdog scheme in the network. Node A first sends out 3-ACK data packet P1 to node B. Then, node B forwards this packet to node X through node C. When node X receives P1, as it is the fourth node in this four-node group, node X is required to send back an S-ACK acknowledgement packet Pk1 to node C. Node C forwards Pk1 back to node A through node B. If node A does not receive this acknowledgement packet within a predefined time period, the node A reports that nodes B, and C are reported as malicious. (Fig 3).The entire acknowledgement scheme helps to avoid sending packets through unreliable routes and inactive nodes in network through verifying mobile node.

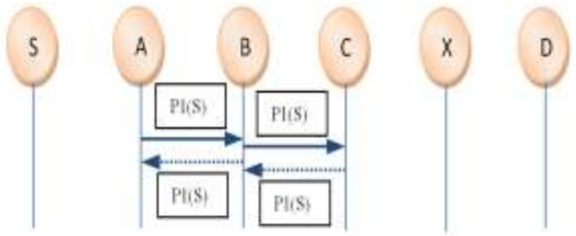

Fig. 2 Two Acknowledgement

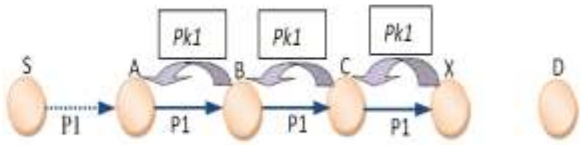

Fig. 3 Three Acknowledgements

III. PROPOSED SYSTEM

In this section we propose selection of most secure and reliable route by implementing the trust value management between two nodes with fuzzy logic rule prediction method. In the proposed scheme each node maintains trust value for its neighbor node. In MANET by using EA3ACK-FA protocol, before packet transmission process compute the trust value, based on trust value compute the route trust and update the trust value in the routing table of the node. If the route is valid route then select most trusted node route then transmit the packets else compute the trust route for the particular packet transmission. The trust value calculated as

Ti (j) = αTi (self) (j) + βTi (neighbor)(j)
Where Ti (j) is the trust of node i on neighbor node j.
Ti (self) (j) represent the trust value of node i on node j.
Ti (neighbor) (j) represent the trust that neighbor of node I has on node j, and α,
β are weighting factor that is α + β = 1.

The neighbor node establishes three structures like to forward and forwarded and source list. To forward store the number of packet to be forwarded and forwarded store the number of packet that are already forwarded and source list define the progenitor of the packet to be forwarded. To forward count of node j is incremented by one when node I find that node j has received the packets which are to be forwarded further. Forwarded count is incremented by one when node j has forwarded that packet which is received. During the packet transmission process the algorithm is, immoral node maintains the source list (S_List) and observes the source packet. Calculate the trust value again. If immoral node fails to update forwarded and To Forwarded count of node j then detect as a malicious node else secure transmission.

```
If [(Forwarded) node j and (S_List Contains Immoral node)]
(Forwarded) node j++;
(To Forward) node j++;
(Forwarded) node j ≥ LimitElse
```

In MANET the nodes energy is consuming when receiving and forwarding data to neighbour nodes. Initially all the nodes have full battery capacity with maximum energy. According to energy consumption the selfish nodes utilize less energy because they only receive data packets they won't forward data packets to neighbors. Whereas the trusted node consuming more energy because they will receive and forward the packets to its neighbors. Each node has different energy calculation based on initial node configuration. The configuration requires following parameters when it's configuring like receive power consumption, transmission power consumption, ideal power consumption. In MANET energy consumption monitored by energy supervisor (EA) for each node when sending and receiving data packets to neighbor. Generally all nodes behave selfish to save battery power without forwarding the packets to the neighbor due to limited resource availability. Energy supervisor monitor packets received by a node, forwarded by a node and battery power affects by each node. Trust value calculated by direct observation of neighbors. In the network every node monitors the behaviour of its neighbors. Every node monitors its neighbor node by using watch dog mechanism whether neighbor node really forward or drop the packets. The neighbor node is monitored by passively observing communication for detecting delayed packet, dropped packet and forward packets. These observations are abnormal action of any node and detect directly to determine the trust value. When communication begins the total trust value (TV) calculated with node index and direct trust value and stored in trust table for each node.

EA = Σ (Packet received + Packet forwarded+ Batter power) / Node

TV = Node index + Direct trust the recommended trust obtaining indirect trust on destination from Node (N).

1. Node Source (S) sends Recommendation Trust Request to node(s) N.
2. If S has direct trust value on D, then it will reply back with Recommendation Trust Reply.
3. Else If S does not have direct trust value record it will discard the Recommendation Trust Request
4. After receiving Recommendation Trust Reply from neighbors consider the trust value of the node with maximum direct trust value by applying fuzzy logic technique.
5. Integrate all the obtained trust value from neighbors to calculate the indirect trust value

To maintain the integrity of the packet communication the modified message by the intermediate node can be discarded. Initially the packet veracity check value (PVC value) is positive, if any modification then PVC value will be decreased. Each message generated by a node includes digital signature through its private key, based on cryptography technique when a node receives a message decrypt using digital signature and public key to authenticate message from neighbor node. Similarly all the intermediate nodes authenticate the message and forward to the neighbor, if any modification in the message content then PVC value will be decremented. In our proposed scheme compared to other asymmetric key algorithms, RSA algorithm is implemented to perform digital signature verification and incur least cost.Final trust value of destination node is calculated with energy value, trust value and packet veracity check value. These values are assigned by each node and generate node trust table for each node. The table contains Node ID, Trust value, Trust type and Trust timeout. The centralized authority node request the final trust manager to recompute the trust value, the trust value of the node gets expired. Every time node trust table updated whenever final trust manager computing trust value, the final trust value is calculated as

FT Value = E value + T value + PVC value

Any node with maximum trust value is elected as certificate authority node. Final trust table helps to certificateauthority to obtain the trust value of each node. Based on certificate authority only the network ensures the secure transmission and segregate the node with in time. Our valuenode get certificate from certified authority else node have to be renewed again. When centralized authority moves out of range then the next maximum trust value elected as a centralized authority node. Source and destination nodes are certified by centralized authority, and then it is eligible for packet transmission. The packet is encrypted using public key from source node and forwards it to the destination. In between packet transmission the intermediate node cannot decrypt and view the message only, the destination node can decrypt the packet using private key and view the message. In the proposed scheme MD4 algorithm used to hash the packet because it is least complex and incurs least energy cost. ISAKMP secure transmission started before the actual transmission between the source and destination node. Source node send request to certified authority node, this certified authority node encrypt it with shared key SKs. After receiving this request certified authority node verifies whether the source and destination nodes are valid and also verify whether the destination in its range. Certified authority nodes generate CERTA and CERTB encrypt with shared key SKs, SKd and forward to source and destination node. Both source and destination node decrypt CERTA and CERTB, make authentication and start communication if certificates are valid. Node reliability increases its trust level, when trust level represents positive experience and node reliability decreases, when trust level represents negative experience. Fuzzy logic has trust values ranging between 0 and 1. The trust values of node can be calculated based on the computed Ev, Tv, PVCv and FTv. These values are the fuzzy input value and node mark as trusted node or malicious node based on fuzzy logic algorithm. When node establishes communication to exchange packet data then fuzzy logic algorithm called automatically. If the fuzzy values falls below a critical threshold value then node marked as malicious. When communication initializes between two nodes, source node sends request to certified authority for certify the node trust value, now fuzzy analyzer is invoked. Fuzzy analyzer verifies the trust level of source node and perform fuzzy table based on fuzzy analyzer algorithm. Certified authority determines the node is TRUSTED or MALICIOUS based on trust value. Certified authority find the requesting node as malicious then generate ALARM message and send to the entire trusted node in its range. Requester node is trusted the certificate authority to generate certificate based on fuzzy based analyzer and sends to the request node. Node makes secure transmission when fuzzy values are VERY HIGH, HIGH and MEDIUM. Node fuzzy values are LOW and VERY LOW is marked as malicious node, certified authority denies certificate for malicious node in the network. When node certificate expired issued by the certificate authority, then trust node send request for renewal of certificate before it starts transmission. The proposed method to solve route traffic and routing delay because of combination of acknowledgements and fuzzy scheme avoided misbehaviour nodes.

Procedural Steps of EA3ACK Algorithm

- EA3ACK processing starts with hybrid cryptography.
- Hello packet transmission from source to destination through intermediate nodes.
- Destination node sends ACK message to source node in same route through intermediate nodes.
- If source node receives this acknowledgement packet within a predefined time period, then data transmission will be start.
- If node A does not receive this acknowledgement packet within a predefined time period, then the intermediate nodes are marked as malicious nodes.
- Switch to S-ACK. Send acknowledgement packet through intermediate node, this model to detect if there are any receiver collision, false misbehaviour nodes and limited transmission power in the route.
- Out of the three consecutive nodes in the S-ACK, the third node is required to send an ACK packet to the temporary source node same rout with opposite direction.
- If node A receives this acknowledgement packet within a predefined time period, then data transmission will be start, otherwise both nodes B and C are reported as malicious.
- Switch to 3-ACK through intermediate node, this model to detect if there are any collision attacks in a route.
- 3-ACK has four consecutive nodes in the route; the fourth node is required to send back ACK acknowledgement packet to the first node.
- If node A receives this acknowledgement packet within a predefined time period, data transmission will be start, otherwise intermediate node is marked as a malicious node, when malicious report is received to the source node than, source node switch to MRA.
- MRA checks authentication (secure value) to all nodes and if MAR receives this acknowledgement packet within a predefined time period, then the data transmission will be start, otherwise marked as misbehaviour node.
- Transmit the data in the alternate path to the destination, and go to step1.

Methodology diagram for EA3ACK-FA

The proposed EA3ACK-FA scheme is described in detail. The approach described in this research is based on the previous work (Shakshuki*et al.* 2013), where the backbone of EA3ACK-FA was proposed and evaluated through implementation. It is extended with the introduction of FA fuzzy approach to prevent the attacker from forging acknowledgement packets and avoided traffic and routing delay. EA3ACK-FA consists of five major parts, namely, ACK, secure ACK (S-ACK), 3-ACK, MRA and FA logic. In order to distinguish different packet types in different schemes in EA3ACK-FA, 3 b of the different types of packets is used. Details of different packet types are listed in Table 1 and a flowchart describing the EA3ACK-FA scheme is presented in Fig. 4 It is to be noted that, in the proposed scheme, it is assumed that the link between each node in the network is bidirectional. Furthermore, for each communication process, both the source node and the destination node are not malicious.

Table 1 Packet Type Indicators

Packet type	**General Data**	**ACK**	**S-ACK**	**3-ACK**	**MAR**
Packet flag	001	010	011	100	101

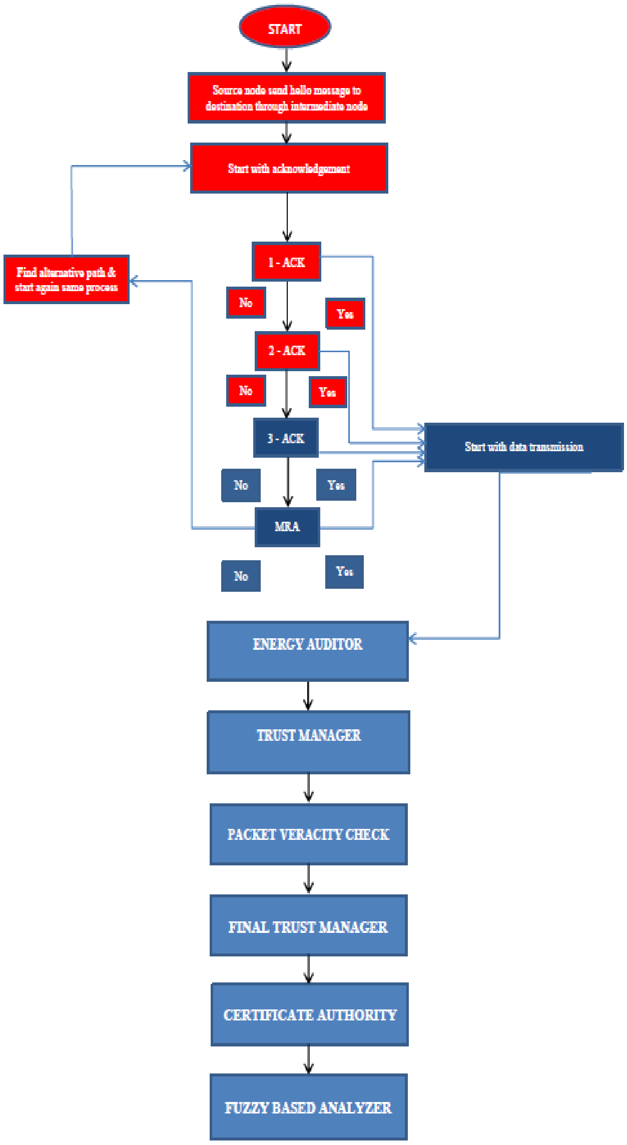
START
Source node send hello message to destination through intermediate node
Start with acknowledgement
Find alternative path & start again same process
1 - ACK
No
Yes
2 - ACK
No
Yes
3 - ACK
No
Yes
MRA
No
Yes
Start with data transmission
ENERGY AUDITOR
TRUST MANAGER
PACKET VERACITY CHECK
FINAL TRUST MANAGER
CERTIFICATE AUTHORITY
FUZZY BASED ANALYZER

Fig. 4 Flow diagram for EA3ACK-FA

The simulation parameters are specified below.

Table 2Simulation Parameters

Parameters	Values
Simulation area	800m * 800m
Number of nodes	70
Average speed of nodes	0–25 m/sec
Mobility model	Random Waypoint
Number of packet senders	50
Transmission range	300m
Constant bit rate	3 (Packets/Second)
Packet size	512 Bytes
Initial energy/node	100 joules
Antenna model	Omni directional
Simulation time	700sec
No. of malicious nodes	14

In this simulation work, it is used to test the IDS's performance when the attackers are smart enough to forge acknowledgement packets and claim positive result while, in fact, it is negative.

IV. PERFORMANCE EVALUATION

Simulation results are obtained by varying the malicious nodes from 10% to 50%. The performances of the proposed EA3ACK-FA and the existing EA3ACK-MARAS, EAACK are compared. Fig. 5 and Table 3 show the proposed EA3ACK-FA with improved packet delivery ratio, when number of malicious nodes is increased from 10% to 50% when compared to the existing methods. It is clear that out of all acknowledgements based IDSs, the proposed scheme EA3ACK-FA surpasses EA3ACK-MARS4 and EAACK (DSA) performance by 12.34% of delivery ratio when malicious nodes 10% to 50% than EAACK (DSA) and average delivery ratio increase by 4.93% of 10% to 50% of malicious nodes than EAACK-MARS4 and average delivery ratio increased in old system of EA3ACK-MARS4 by 7.79% of 10% to 50% of malicious nodes than EAACK(DSA). From the results, it is concluded that the acknowledgement based scheme, EA3ACK-FA, is able to detect malicious in the presence of receiver collision, limited transmission power, and false misbehaviour report and collusion attacks, all the packet will be communicated with authenticated using fuzzy logic.

Table 3 Packet Delivery Ratio Vs Malicious Nodes

Packet Delivery Ratio					
Routing / Malicious Node	**10%**	**20 %**	**30 %**	**40 %**	**50 %**
EAACK(DSA) (Shakshuki*et al.* 2013)	0.81	0.76	0.71	0.66	0.61
EAACK-MARS4 ((Thamizhmaran*et al 2017*)	0.87	0.82	0.77	0.72	0.67
EA3ACK-FA	0.91	0.86	0.81	0.76	0.71

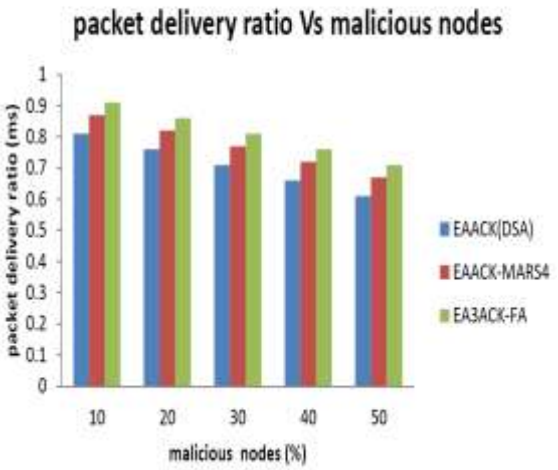

Fig. 5 Malicious Nodes Vs Packet Delivery Ratio

Fig. 6 and Table 4 compare the routing overhead performance of the proposed EA3ACK-FA and existing acknowledgement based IDS schemes. EA3ACK-FA has reduced routing overhead with the number of malicious nodes from 10% to 50% when compared to the existing methods as show in Fig. 6. Suggested new method has the reduce average routing overhead by 17% than EAACK-MARS4,38.9% than EAACK (DSA) of 50% of malicious nodes and EA3ACK-MARS4 routing overhead reduced 18% then EAACK(DSA) with overall malicious nodes varied 10% to 50%, although EA3ACK-FA requires for learning update at all acknowledgement process. Because designed to frame proposed model to avoid path selection without malicious nodes, so number of selected path will be reduces.

Table 4 Routing Overhead Vs Malicious Nodes

Routing Overhead					
Routing / Malicious Node	**10%**	**20%**	**30%**	**40%**	**50%**
EAACK(DSA) (Shakshuki*et al.* 2013)	0.24	0.31	0.38	0.45	0.50
EAACK-MARS4 ((Thamizhmaran*et al 2017*)	0.18	0.25	0.32	0.39	0.44
EA3ACK-FA	0.13	0.20	0.27	0.34	0.41

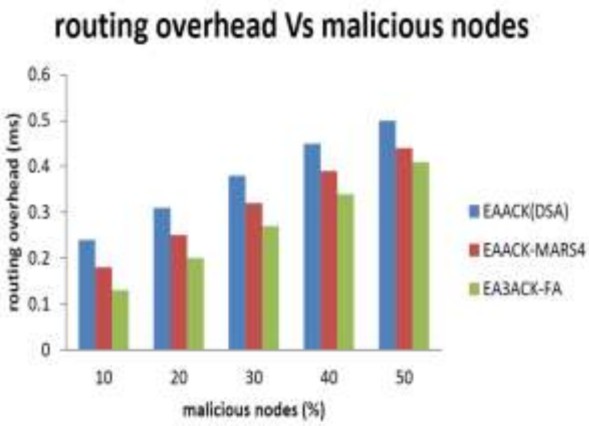

Fig. 6 Malicious Nodes Vs Routing Overhead

Fig. 7 and Table 5 compare the throughput performance using three algorithms. Result of Fig. 7 shows that suggested concept has well improved performance of average throughput by 21.51% with the number of malicious nodes 50% compared to the EAACK-MARS4, increase average throughput by 45.94% than EAACK (DSA) acknowledgement schemes with malicious nodes 10%. It is clear that the existing technic EA3ACK(DSA) decreases the average throughput by 18.98% then proposed new model with increasing malicious nodes 10% to 50%. Proposed algorithm to increases number of active nodes and to identify avoid malicious nodes, it is capable of finding the minimum link failed unbreakable short route between the source to destination and also increase number of successfully deliver packets without malicious node than existing methods due to FA better than MARS4 and DSA. New method increase number of active packets successful delivery due to using fuzzy approach technics than existing method

Table 5 Throughput Vs Malicious Nodes

Throughput					
Routing / Malicious Node 0%	**10%**	**20%**	**30%**	**40%**	**50%**
EAACK(DSA) (Shakshuki*et al.* 2013)	0.20	0.23	0.36	0.49	0.62
EAACK-MARS4 ((Thamizhmaran*et al 2017*)	0.32	0.35	0.48	0.61	0.74
EA3ACK-FA	0.37	0.40	0.53	0.66	0.79

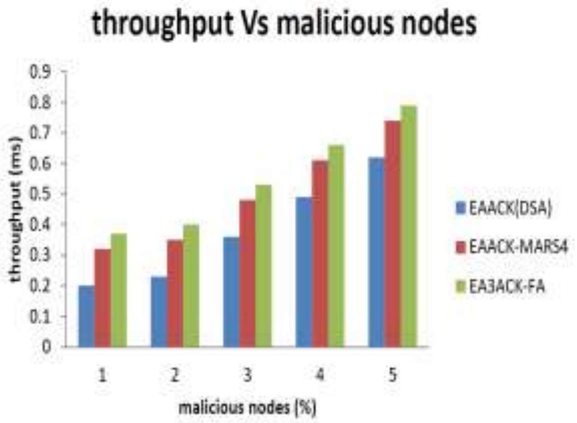

Fig. 7 Malicious Nodes Vs Throughput

Fig. 8 and Table 6 compare the remaining energy of the proposed EA3ACK-FA and the existing EA3ACK-MARS4, EAACK (DSA). Fig. 8 shows that suggested system reduces remaining energy when the number of malicious nodes varied compared to the existing system. It is clear that the existing technic EA3ACK-MARS4 decreases the average remaining energy by 9.86% then proposed new model with increasing malicious nodes 10% to 50% and EA3ACK-FA model increased remaining energy by 19.45% then EAACK (DSA) with increasing malicious nodes 10% to 50% and also EA3ACK-MARS4 model increased remaining energy by 10.29% then EAACK (DSA) with increasing malicious nodes 10% to 50%, due to increases duration of time period of three acknowledgments than two acknowledgments it is possible to decrease remaining energy, because of increase acknowledgements, to take some time to reach destination it is possible to increase remaining energy.

Table 6 Remaining Energy Vs Malicious Nodes

Remaining Energy					
Routing / Malicious Node	**10 %**	**20 %**	**30 %**	**40 %**	**50 %**
EAACK(DSA) (Shakshuki*et al.* 2013)	0.76	0.70	0.54	0.50	0.44
EAACK-MARS4 ((Thamizhmaran*et al 2017*)	0.83	0.77	0.61	0.57	0.51
EA3ACK-FA	0.91	0.85	0.69	0.63	0.57

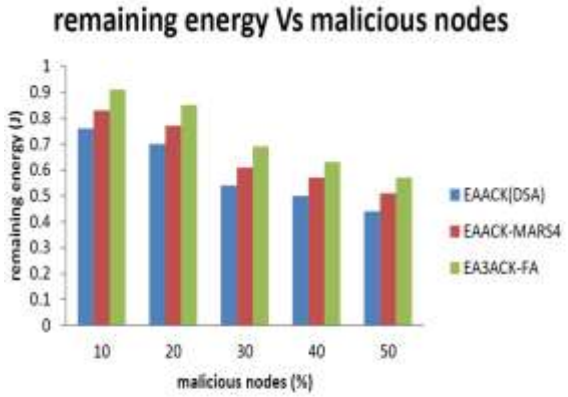

Fig. 8 Malicious Nodes Vs Remaining Energy

From all the above figures and tables it is clear that the comparison of the proposed EA3ACK-FA with the conventional routing protocol and other existing acknowledgement based IDS schemes, shows the packet deliver ratio, throughput and remaining energy increase and routing overhead decrease with the increase in the number of malicious nodes.

V. CONCLUSION

Acknowledgement based transmission becomes essential and is very safe with high security. In this research, a proposed routing protocol named EA3ACK-FA is proposed with technic fuzzy logic (FA). The simulation results propose EA3ACK-FA algorithm as compared with the existing EAACK-MARS4 and EAACK(DSA) algorithm through the network simulation 2. This new developed model ability to detect misbehaviour nodes with improves average packet delivery ratio by 12.34% of delivery ratio than EAACK (DSA), average delivery ratio increase by 4.93% than EAACK-MARS4 and average delivery ratio increased in old system of EA3ACK-MARS4 by 7.79% than EAACK (DSA) with number of malicious nodes increased 10% to 50%. EA3ACK-FA has reduce average routing overhead by 17% than EAACK-MARS4, 38.9% than EAACK (DSA) of 50% of malicious nodes and EA3ACK-MARS4 routing overhead reduced 18% then EAACK(DSA) with malicious nodes varied 10% to 50%. Suggested proposed concept has well improved performance of average throughput by 21.51% with the number of malicious nodes 50% compared to the EAACK-MARS4, increase average throughput by 45.94% than EAACK (DSA) acknowledgement schemes with malicious nodes 10%. It is clear that the existing technic EA3ACK (DSA) decreases the average throughput by 18.98% then proposed new model with increasing malicious nodes 10% to 50%, it is clear that the existing technic EA3ACK-MARS4 decreases the average remaining energy by 9.86% then proposed new model with increasing malicious nodes 10% to 50%. EA3ACK-FA model increased remaining energy by 19.45% then EAACK (DSA) with increasing malicious nodes 10% to 50% and EA3ACK-MARS4 model increased remaining energy by 10.29% then EAACK (DSA) with increasing malicious nodes 10% to 50%. Finally EA3ACK-FA not only reduces overhead, but also solves key exchange problem using FA algorithm.It is suggested that further experiments are necessary to compare the secure transmission of different routing algorithms. However, most of the existing routing algorithms proposed for MANET are not fault tolerant. To enhance the merits of this research work, there is a plan to investigate the following issues in future.The same concept can be applied in satellites to reduce overhead, delay and also increasing remaining energy in the route and testing the performance of EA3ACK-FA, EA3ACK-MARS4, EE-EA3ACK and SHSP-EA3ACK in real time network environment.

Reference

[1] AbdulsalamBasabaaa., Sheltamia, Tarek., and Shakshuki, Elhadi., (2014), Implementation of A3ACKs Intrusion Detection System Under Various Mobility Speeds, Proceedings Of 5th International Conference on Ambient System, Networking Technologies, Hasselt, Belgium, June, 571–578.

[2] Basagni, S., Conti, M., Giordano, S., and Stojmenovic, I.,Mobile ad hoc Networking, First edition, Wiley-IEEE Press, New Jersey, 2004.

[3] Burmester, M. and de Medeiros, B. (2009),On the Security of Route Discovery in MANETs, IEEE Transactions on Mobile Computing, Vol. 8(9), pp. 1180–1188.

[4] Denning, D. (1987),An Intrusion Detection Model, IEEE Transactions on Software Engineering, Vol. 13(2), pp. 22-39.

[5] Grossglauser, M. and Tse, D. (2002), Mobility Increases the Capacity of Ad hoc Wireless Networks, IEEE Transactions on Networking, Vol. 10(4), pp. 477–486.

[6] Hui Xia., Jia Yu., Zhen-kuan Pan., Xiang-guo Cheng., and Sha., (2016), Applying Trust Enhancements to Reactive Routing Protocols in MANETs, Wireless Communication, Vol. 22(7), pp. 2239-2257.

[7] Jian-Ming Chang, and Po-Chun Tsou., Isaac Woungang., and Han-Chieh Chao., (2014), Defending Against Collaborative Attacks by Malicious Nodes in MANETs: A Cooperative Bait Detection Approach, IEEE Systems Journal,Vol. 9(1), pp. 65–75.

[8] Nan Kang., Shakshuki, Elhadi M., and Sheltami, Tarek R., (2010), Detecting Misbehaving Nodes in MANETs, ACM Proceedings of 8th International Conference on Advances in Mobile Computing and Multimedia,Paris, France, August, 1-7.

[9] Nan Kang., Shakshuki, Elhadi M., and Sheltami, Tarek R., (2011), Detecting Forged Acknowledgements in MANETs, proceedings of 25th International Conference on Advanced Information Networking and Applications,Biopolis, Singapore, March, 488-494.

[10] Peng Zhang., Chuang Lin., Yixin Jiang., Yanfei Fan., and XueminShen., (2009), A Lightweight Encryption Scheme for Network-Coded MANETs, IEEE Transactions on Parallel & Distributed Systems,Vol. 24(4), pp. 1-6.

[11] Saaidal Razalli Azzuhri., Harith Ahmad., Marius Portmann., Ismail Ahmedy., and Rainhard Dieter Findling., Muhammad Muaaz., Daniel Hintze., and Rene Mayrhofer., (2017), Shake Unlock: Securely Transfer Authentication States Between Mobile Devices, IEEE Transactions on Mobile Computing,Vol.16(4),1163-1175.

[12] Sethi, et al (2011) “Fuzzy-based trusted ant routing (FTAR) protocol in mobile ad hoc networks", Multi-disciplinary Trends in Artificial Intelligence, Springer, pp. 112-123.

[13] Shakshuki, Elhadi M., Nan Kang., and Sheltami, Tarek R., (2013), EAACK—A Secure Intrusion-Detection System for MANETs, IEEE Transactions on Industrial Electronics, Vol. 60(3), pp. 1089-1098.

[14] Wang, X. and Li, J. (2013), Improving the Network Lifetime of MANETs Through Cooperative MAC Protocol Design,

IEEE Transactions on Parallel and Distributed Systems, Vol. 99(1), pp. 1-11.

[15] Yang, H., Luo, H., Ye, F., Lu, S., and Zhang, L., (2002), Security in Mobile Ad hoc Networks: Challenges and Solutions, IEEE Wireless Communications, Vol. 11(1), pp. 38–47.

[16] Yu Zhang., LoukasLazos., and William Kozma., (2012), AMD: Audit-Based Misbehavior Detection in Wireless Ad hoc Networks, IEEE Transactions on Mobile Computing, Vol. 15(8), pp. 1893–1907.