Modelling and Mitigation of various secure routing technique in Manets

Author Ritu[1], Author Sourabh Aggarwal[2]

(E-mail: ritugarg101@gmail.com)
(Email: singla.saurabh249@gmail.com)

Abstract—Mobile ad hoc networks (MANETs) are automatically deployed over a geographically limited area without well-established infrastructure. The networks can work well only if the mobile nodes are trusty and they behave cooperatively. Due to the frankness in network topology, MANETs are very vulnerable to various attacks from malicious nodes. Hence, providing safe communication is a major research area in MANETs. The autonomous systems of wireless mobile nodes can be set up anywhere and anytime. However, due to high mobility, absence of centralized authority and open media nature, MANETs are more exposed to various security threats. As a result, they are susceptible to more security issues as compared to the traditional networks. Ad hoc networks are highly prone to various types of attacks such as active and passive attacks. Sequence number attacks are such high-risk attacks which greatly decrease the performance of the network. Sequence number attacks gasp some or all data packets and after that ditch them. In past few years, various researchers proposed different solutions for finding the sequence number attacks. In this paper, we stated all related works done by various researchers those provide to detect sequence number attacks to secure the ad hoc network. The review entirely presents distinct facet of the proposed approach.

Keywords—*Mobile Ad hoc network; Secure routing; Sequence number; attacks; Proactive scheme; Linear Regression;*

I. Introduction

MANET stands for Mobile ad hoc Network. It is also called as wireless ad-hoc network or ad-hoc wireless network that usually has a routable networking environment on top of a Link Layer ad-hoc network. They contain a set of mobile nodes connected wirelessly in a self-configured, self-healing network without having a fixed infrastructure [1]. MANET nodes are free to move randomly as the network topology changes routinely. Each node acts as a router as they redirect traffic to other specified node in the network [2]. MANET can be the part of a large internet. They form extremely effective autonomous topology with the presence of one or multiple different transceivers between nodes. Wireless links usually have lower reliability, efficiency, stability and capacity as compared to wired network. The throughput of wireless communication is even less than a radio's most of the transmission rate after dealing with the constraints like multiple access, noise, interference conditions, etc. Each node can act as a host and router, which shows its autonomous behavior. Some or all the nodes depend on batteries or other finite means for their energy. Mobile nodes are characterized with less memory, power and light weight features. Wireless network is more susceptible to security threats. A centralized firewall is absent because of its distributed nature of operation for security, routing and host configuration. They need minimum human intervention to configure the network, therefore they are effectively autonomous in nature.

The main challenge for the MANET is to enable each device to continuously maintain the information required to properly route traffic [3,4]. MANETs have a peer-to-peer, self-forming, self-healing network MANET's circa 2000-2015 typically communicate at radio frequencies (30MHz-5GHz). This can be applied in road safety, ranging from sensors for environment, home, health, disaster rescue operations, air/land/navy defense, weapons, robots, etc.

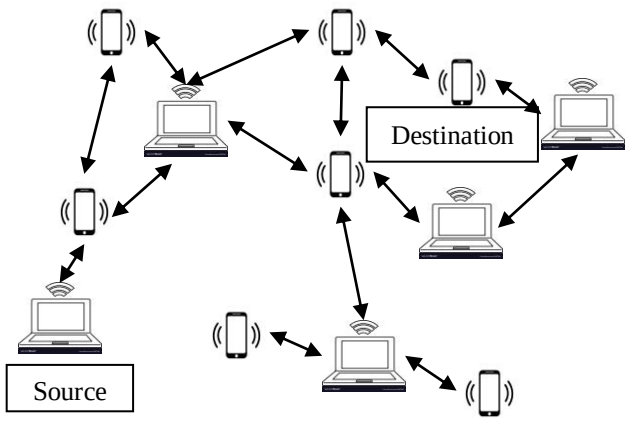


Fig 1: Mobile Ad-hoc Network

The rest of the paper is organized as follows: Section 2 represents why security is needed in the ad hoc networks. Section 3 describes the existing schemes addressing routing security of ad hoc networks. Section 4 discusses about the how sequence number affects the network. Section 5describes the concept of linear regression. Section 6discusses our proposed

solution to mitigate the effect of sequence number attack and finally, Section 7concludes the paper.

II. Why security is needed

Security has become a major research area due to their applications in the field of ad-hoc networks. Establishment of a secure path between source and destination nodes is vital in order to communicate smoothly in the entire network. High mobility and lack of fixed infrastructure causes new security problems as a result, they are prone to more security issues as compared to the traditional networks. Ad hoc networks are highly susceptible to various types of attacks such as active and passive attacks Therefore, securing a MANET is a challenging issue which needs to be understand the possible forms of attacks [5].

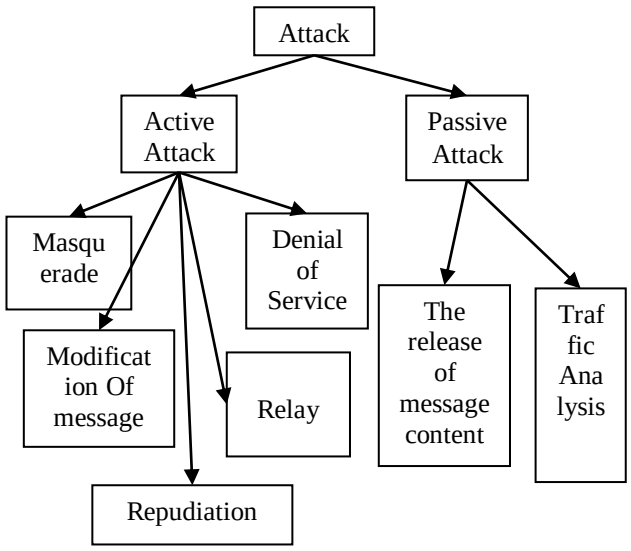


Fig 2: Types of Attack

***Active Attacks*-**An Active attack aims to change system resources or effect their operations. Active attacks cause some alteration of the data stream or creation of fake statement. It involves actions such as duplication, alteration or elimination of exchanged data. Types of active attacks are as following:

- *Masquerade*–Masquerade attack takes place where one entity pretends to be different entity.
- *Modification of messages*–It means that some portion of a message is changed or that message is delayed or reordered to produce an unlicensed effect. For example, a message meaning "Allow JOE to read confidential file A" is modified as "Allow Siya to read confidential file A".
- *Repudiation*–This attack is done by either sender or receiver. The sender or receiver can negate later that he/she has send or receive a message. For example, customer ask his Bank "To transfer an amount to siya" and later on the sender(customer) deny that he had made such a request. This is an example of repudiation.
- *Replay*–It involves the passive capture of a message and its subsequent the transmission to produce an authorized effect.
- *Denial of Service*–It prevents normal use of communication facilities. This attack may have a specific target. For example, an entity may conquer all messages directed to a particular destination. Another form of service denial is the disruption of an entire network with her by disabling the network or by overloading it by messages so as to degrade performance.

***Passive Attacks*-**A Passive attack aims to learn or make use of information from the system but it does not infect system resources. Passive attacks do not interrupt the operations of a protocol; they only gather the information by noticing of the network in order to introduce active attacks in future. Types of Passive attacks are as following:

- *The release of message content*–Telephonic conversation, an electronic mail message or a transferred file may have sensitive or confidential information. We would like to prohibit an opponent from observing the contents of these transmissions.
- *Traffic analysis*–Assume that we had a way of masking (encryption) of information, so that the attacker even if captured the message could not extract any information from the message. The opponent could govern the location and name of communicating host and could identify the frequency and length of messages being exchanged. This information might be helpful in considering the nature of the communication that was taking place.

Sequence number attacks which are a well-known threat on the network layer of MANETs. Sequence number attack is type of Denial-of-Service attack. This is an important attack on Ad hoc on-demand distance vector (AODV) and Dynamic Source Routing (DSR). AODV maintains routes by with the concept of sequence numbers. Freshness of a route is determined by destination sequence number's value. It means higher sequence number decides the path of data forwarding [6]. A malicious node introducing sequence number attack with a fake path reply packet with higher sequence number and lower hop count in order to construct a forged path. Once the path gets constructed, malicious node can drop packets coming from particular destination or for particular timeduration or drops packet randomly [7]. This reduces the performance of a network by affecting Quality-of-Services.

III. Literature Review

In the practical implementations of the MANETs, Security is a main area of concern. In recent years, many researchers have proposed different predictive schemes to

improve the routing security in MANETs which is reviewed in this section. Summary of the same is described in Table 1.

Alheeti et al. [8] introduced intrusion detection and prediction technique for detecting denial-of-service (DoS) and blackhole attacks in vehicular ad-hoc networks (VANETs). The technique is devised to secure the external communication in self-driving and semi self-driving vehicles. This technique is based on the Linear Discriminate Analysis (LDA) and Quadratic Discriminate Analysis (QDA) to forecast the attack based on the observations of vehicles' behavior. Fuzzification of data is carried out for generating final results which shows behavior of different nodes. After identifying malicious or abnormal behavior, mobility and traffic scenarios are generated.

Singh et al. [9] introduced an intrusion detection and prevention system which is used for detecting malicious nodes in MANETs. This trust-based mechanism discovers malicious nodes by behavior classifier on the basis of predefine threshold and risk factor conditions. Direct and indirect trust values are used to compute the aggregated trust value. A risk factor is computed using these two trust components.

Gundluru et al. [10] introduced a Trust based Framework for Group Key Management which is aimed to consume less computing power and to secure MANETs against internal as well as external attacks. It retains the energy of a wireless node by adopting the game theory strategy which finds an optimal set of remote nodes to send a trust request. After trust computation, a fuzzy concept is approved in order to get the degree of trustworthiness instead of binary classification. It uses clustering approach in which a cluster leader is chose for each cluster. Cluster leader periodically forecasts the trust value based on fuzzy rule by direct and indirect observations. Indirect trust is calculated by observing responses of trust requests from all those neighbor nodes whose trust value is above the threshold value.

Dhananjayan et al. [11] devised a Trust-aware Ad hoc Routing (T2AR) protocol which computes the trust level between the nodes in the MANET and performs a secure data transmission between nodes. It forecasts a trust value based on energy, mobility, and RSSI based distance measurement. This protocol acquires the information from neighbor to report the success and failure rate of packet transmission. The trust value is calculated based on the packet sequence ID matched with log reports of the node. Hence, in the proposed work, the trust value is calculated through estimation of energy, the success rate of packets delivery and mobility. The direct computation of trust value is carried out using a Bayesian framework by observation of the nodes.

Muthuramalingam et al. [12] devised a scheme which is used to investigate network security by calculating trust value using direct and indirect observations. To compute the trust value with direct observations, full probability-based Bayesian interface is used while with indirect observations, neighbor hop based information is used. To compute the final trust value, Dempster-Shafter theory using both direct and indirect trust values is used. Also, Dijkstra's shortest path algorithm is used for searching the shortest route between nodes in the network.

Babu et al. [13] introduced a scheme that is used to identify data replacement attack and false notification attack in MANETs. The introduced method detects these attacks by using a score value in top k query processing. It broadcasts false notification information to all other nodes to circulate information abo0ut malicious nodes in the network. A node sends its own forecasted score value along with a path value to decide a particular path to send data.

Manoharan et al. [14] proposed an Erlang Coefficient based Conditional Probabilistic Model for insulating selfish nodes through the manipulation of Conditional Probabilistic Coefficient (CPC) factor. This factor acts as reputation factor for calculating negative effect produced by selfish nodes. In this model, three steps are performed. In the first step, the identification of selfish node is carried out based on a genius factor. Genius factor is forecasted by neighbor nodes using packet forwarding and receiving rates. In the second step, a computation of a non-cooperative factor is carried out. This factor based on the number of selfish nodes present in a routing path between source and destination nodes. Selfish nodes are detected by the above Genius factor. In the third step, determination of CPC is performed depends on Erlang Distribution. This approach forecasts the failure rate of cooperative nodes. This approach based on two independent exponential random variables. Depend on these three steps, it insulates selfish nodes in the routing path.

Li et al. [15] introduced an Attack-Resistant Trust Management Scheme which is used to identify malicious nodes and to evaluate trustworthiness of data in VANETs. In this scheme, data trust is forecasted on the basis of data sensed from multiple vehicles. Trust is determined in two dimensions viz. functional trust and recommendation trust. This scheme works in two steps: data analysis and trust management. In data analysis, it collects traffic data from different vehicle nodes and using Dempster-Shafer theory; using probability and belief of nodes the collected data gives an evidence. In trust management, recommendations and predictions of the vehicle nodes are considered.

Rathnamma et al. [16] proposed a plan to provide trust based secure routing in MANETs. Four types of trust are computed and depends on that energy of the nodes is computed. In the first type, initial trust is assumed which gives same priory to all the nodes by giving them initial trust value. In the second type, behavioral trust is computed depends on behaviors of the nodes. In the third type, neighbor trust computed based on direct and indirect trust components. Finally, depends on all these three types, a final trust value is calculated.

Kumar et al. [17] introduced a strategy for spotting the resource constrained mobile nodes in MANETs. In this scheme, a centralized environment is organized using groups and subgroups. Probability analysis of distance bounding protocol reveals that the proposed approach protects network from mafia fraud, distance fraud, terrorist fraud and distance hijacking attacks. In the performance analysis, it uses Zone

Routing Protocol (ZRP) which is used to issue an efficient and secure route. For lightweight grouping, it implements collection of node information and propagation of the information. Once the subgroup is generated, protection from various attacks and relationship maintenance are carried out by a trust model. The trust management contains trust generation, trust propagation, trust accumulation, trust prediction and trust application.

Sengathir et al. [18] proposed an Exponential Reliability Coefficient based Reputation Mechanism (ERCRM), in which the selfish nodes are insulated from the routing path using an exponential reliability coefficient (ExRC). Reliability of coefficient is operated using the parameters such as failure rate and residual energy of nodes. The moving average method is used for quantifying the reputation level of mobile nodes through which decision insulation is carried out. Estimation of the energy level of intermediate nodes in the routing path considers two parameters, the residual power and power drain rate. The scheme forecasts a value using the energy level, which is based on the matrix to increase security and reliability of the network.

Poongodi et al. [19] introduced a scheme which uses Truth Convergence based Aumann Agreement Theorem for observation and prevention of attacks in MANETs. It brings out the behavior of nodes and identifies its patterns. Based on that, it predicts the future attacks in the network. It uses searching Truth Convergence based confidence value which identifies false positives and false negatives in terms of malicious behavior of the nodes. A trust value is determined based on direct observations with Bayesian inference using uncertainty reasoning. After that, a voting-based intrusion detection system is used for defining compromised and uncompromised goal nodes in the system. Aumann Agreement theorem is used to compute the truth and confidence values of nodes in the network. Group keys are generated time to time for all the nodes and rekeying protocols are used to provide confidentiality in the network.

Patel et al. [20] proposed a scheme, used for providing security to identify and detect gray hole attack in both phases that is route discovery and route transmission phase. In route discovery phase first, it check node sequence number with routing table sequence number if node sequence number beat to the routing table sequence number then packet accept otherwise reject that packet. After that in data transmission phase each node maintains threshold value. If threshold value of that node beat to the node sequence number than discard that reply packet. Otherwise check that receiving node source node or not. If node source node then free reply packet and start data transmission. Otherwise forward reply packet in reverse path towards source node. Here calculation of threshold value done on base of routing table sequence number, number of data packet send from node and number of data packet receive from node.

Sengathir et al. [21] introduced an Advanced Trust Coefficient based Semi Markov Prediction Model to explore the effect of selfish nodes in MANETs. The Semi-Markov Prediction model states the lower and upper bound of network survivability. It identifies and isolates the selfish nodes from the routing path depends on an innovative trust coefficient. In this model, first random properties of mobile nodes are computed. For this computation, it uses input parameters of source and destination nodes and then, it computes the model parameter. For the model parameter, it finds probability of a node to become selfish or failure node. Using this behavior of model, it defines a probabilistic matrix. After that, using a Semi- Markov model the advanced behavior of a node is estimated and, based on that, insulation of a selfish node is carriedout.

Priyadarshini et al. [22] devised a scheme called Energy and Mobility based Group Key Management which focuses on cluster formation, link stability, mobility prediction and group key management in MANETs. In this scheme, cluster formation is carried out using identification of transmission range. For identification of transmission range, Hello messages are broadcasted to next hop nodes. Link stability is calculated by metrics of received power and distance between nodes. Mobility prediction is carried out by analyzing different patterns of connectivity. Next value of time series is forecasted using previous position of node which is analyzed with an auto regression technique. For a group key generation, a random bit algorithm is used. In this method, a random unique ID is provided to all the nodes.

Wang et al. [23] proposed energy efficient group key management protocol that is used for energy efficient security, scalability, key establishment and key distribution in a network. In this protocol, three functionalities are conducted for security and energy efficiency in the network. For creating a group, notice the neighbor nodes and then forecast the quality of the link between them. After creating a group, second functionality is conducted to provide key for a group using Diffie-Hellman protocol. Third functionality is a strategic mobile management mechanism which is used for handling the mobility effects to boost the multicast energy efficient and secret communication among roaming users.

Senthil Kumar et al. [24] introduced a scheme which is used to identify dishonest nodes in MANETs. Trust value of a node is forecasted based on its past behaviors by using fuzzy logic rule prediction. A trusted path is discovered using trust based source routing. A trust management model is splited

into two parts: subjective evaluation model and trusted routing model. In the subjective evaluation model, a trust value is computed based on trustworthiness of nodes. Based on the analytic hierarchy process, decision about the nodes and their future behaviors are forecasted. This decision and prediction are used to insulate untrustworthy nodes and to organize a secure route towards the destination.

Xia et al. [25] proposed a scheme used for identifying malicious nodes. To identifying malicious node, it used fuzzy based trust prediction mechanism. For that it uses a historical trust and compute current trust of node. Depends on that fuzzy define the degree of trustworthiness of nodes. Based on that, define secure path using trust based secure routing protocol. In this scheme first dynamic prediction model used for predict the trustworthiness of node. Here prediction of trustworthiness of node performs using node historical behavior. Based on historical behavior it computes the current node behavior on that basis it define node malicious or not. To define node malicious behavior, it used fuzzy based prediction model and forecast that node malicious or not. After that using trust based secure path based on application it define the shortest and trusted path for data packet transmission. Here node trusted or not decided depends on data and control packet of node. However, the reviewed proactive approaches are based on pure heuristics while the reactive approaches compromise the QoS, specially for critical applications when deadlines are important

TABLE 1: Literature Review

Title	Methodology	Objective	Performance metrics	Future scope
Using Discriminate Analysis to Detect Intrusions in External Communication of Self-Driving Vehicles [8]	Linear and Quadratic Discriminate Analysis, Fuzzification of the data	Identifying and preventing attacks such a denial of service(dos) attack using historical data in VANET	False positive rate, true positive rate, packet delivery ratio, average throughput, average end-to-end delay	Enhance road side unit with Intelligent IDS and Vehicles with AI techniques
An Intelligent Intrusion Detection and Prevention System for Safeguard Mobile Adhoc Networks Against Malicious Nodes [9]	Risk Factor Calculation	Detection and Prevention of attacks such as black hole, flooding, selective packet drop using a trust manager in a route	Packet loss, Throughput, Overhead, End-to-End Delay	Utilizing the properties of Fuzzy membership functions or data mining techniques for detecting different attack
Soft-computing Based Trust Management Framework for Group Key Management in Manets [10]	Group Key management, Trust management Framework(TMF), Game theory and Fuzzy logic	Isolating internal as well as externalizing fuzzy concept in order to get the degree of trustworthiness	Packet delivery ratio, packet loss, Average residual energy, detection ratio of malicious nodes, key management overhead	Investigate various issues and defiance mechanisms for attacks such as bad-mouthing, ballot-tufting, and collusion
T2AR: trust-aware ad-hoc routing protocols for MANET [11]	Neighbor log collection Neighborhood, Trust rate computation, Energy estimation	Determination of malicious node on basis of energy and mobility	packet delivery ration, throughput, average end to end delay	Security enhancement using location key management protocol

Title	Methodology	Objective	Performance metrics	Future scope
Enhancing the Security for MANETs by identifying untrusted Nodes using Uncertainty Rules. [12]	Bayesian interface, Dempster-Shafter theory observation Scheme, The Dijkstra's algorithm	Isolate the misbehaving nodes from the routing path by predicting trust between nodes	Packet delivery ratio, packet delay, throughput	Devising trust based method with classification
An effective Attack elimination method for Top-K Query processing in MANETs [13]	Top k query-based trust framework	Detection of data replacement attack and false notification attack by predicting the score value with query processing	Query Result accuracy, traffic flow analysis	Using a trust-based system which also predicts trust value
Erlang coefficient based conditional probabilistic model for reliable data dissemination in MANETs [14]	Erlang coefficient based Conditional probabilistic model, estimation of Genuineness Factor, estimation of non-cooperatively	Isolating the selfish node by using condition Probability coefficient factor	Packet delivery ratio, throughput, total overhead, control overhead	Reputation based mechanism can be developed isolate selfish nodes
ART: An Attack-Resistant Trust Management Scheme for Securing Vehicular Ad hoc Networks. [15]	Attack-Resistant Trust management Scheme (ART) For VANETs, update of local evidence for node using the Dempster-Shafer Theory (DST)	Detecting attacks in VANET by evaluating trustworthiness of data	perception rate	Developing a query based GloMoSim
A relationship-based approach for energy aware secure routing in MANETs [16]	Trust management Scheme based on relationship	Determining and isolating misbehaving nodes using prediction of trust rate	Packet delivery ration, throughput, end-to-end delivery	Develop a mechanism which allows malicious nodes to become a trusted node again
Design and Analysis of Light Weigh Trust Mechanism for Secret Data using Light weight [17]	Lightweight Identification, Grouping and trust Based distance bounding	Predicting MANETs against them Fraud, distance fraud, terrorist fraud, and distance	Delivery ratio, good input, energy consumption, jitter	Using Fuzzy method to predict trust value
Exponential reliability coefficient based reputation mechanism for isolating selfish node in MANETS [18]	Exponential reliability coefficient based reputation mechanism (ERCRM)	Improving the reliability of network by isolating selfish nodes	Packet delivery ratio, throughput, control overhead, total overhead	Reputation based mitigation mechanisms that incorporate kappa and Cronbach's statistical coefficient for identifying selfishness behavior of mobile nodes

Title	Methodology	Objective	Performance metrics	Future scope
Detection and Prevention System towards the Truth of Convergence on decision using Aumann agreement Theorem [19]	Truth Convergence Based Aumann agreement Theorem	Detection and prevention of dos attack by identify the behavior of a node	Detection range, Packet delivery Ration	Trust estimation with bound of confidence in a multi-relay access network with heterogeneous environment
Dual Security Against Gray hole Attack in MANETs [20]	Dual security based Approach	Detecting and identifying gray hole attack in MANETs	Packet drop ratio	Perform predictive approach using other techniques
A Futuristic trust coefficient-based semi-Marko prediction model for mitigating selfish node in MANETs [21]	Futuristic trust coefficient-based semi-Marko prediction model, Validation of FTCSPM model	Investigating and quantifying the impact of selfish behavior in survivability of network	packet delivery ratio, energy consumption ration, average end-to-end delay, packet drop rate, throughput	Developing semi Markov prediction model based on pure birth–death process
Energy and Mobility Based Group Key Management in Mobile Ad Hoc Networks [22]	Energy and Mobility based Group Key Management	Secure MANETs with group key management by predicting the mobility of nodes	time taken for key generation, overhead, average no of clusters &key updating, average energy consumption, average no of key updating	Work on Real time application such as database application and web-based application
The energy-efficient Group key management protocol for strategic mobile scenario of MANETs [23]	Group establishment algorithm for strategic mobile scenario, Diffie-Hellman group key management	Efficient detection and predicate the quality of a link on basis of time slot to make a group and assigning a group key	Computational complexity	Selection of routing path using a more technique and enhancing clustering technique
Modified TSR protocol to Support trust in MANET [24]	Trust management model and Trust routing model	Elimination of malicious node to obtain reliable packet delivery	Packet delivery ratio, throughput, overhead ,latency	Developing techniques for efficient energy consumption
Ad-Hoc Networks Trust prediction and trust based source routing in mobile adhoc networks [25]	Authentication Trust based source routing using fuzzy based prediction	Hijacking attack Identifying and isolating the misbehavior	Packet delivery ratio, network throughput	Determination optimal route can be based on quality of service, load and delay

IV. How Sequence Number Affects

Reactive protocols such as AODV are susceptible to sequence number attacks because of friendly environment during their development. We indicate RQ notation to the route request packet (RREQ) and RP notation to the route reply packet (RREP) of AODV. Consider a MANET setup adopting AODV protocol as shown in Fig. 3a (consider Table 3 for Fig. 3), a source node S wants to communicate with a destination node D. It transmits RQ1 with last known destination sequence number 16, which is received by the neighbor nodes A and B in its communication range.

The received packets are retransmitted again by the receiving node A and B as RQ4 and RQ2 to their connecting nodes.The process carries on until a node having fresher route or the destination itself receives the request. Assuming the destination D receives the RQ4 from node A. Meantime, node C has also sends RQ3 to D. However, the destination D drops RQ3 from node C and forwards RP1 on the reverse path to the source node S with sequence number value 20 via D-A-S. The source node S now establishes route S-A-D to transfer data packets as shown in Fig. 3b.

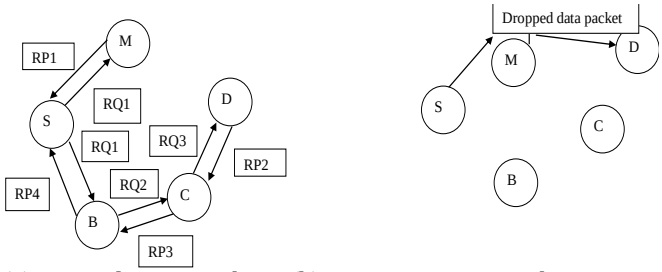
(a)Route discovery phase (b) Data transmission phase

Fig 3: Route discovery and data transmission in AODV [6]

TABLE 2: RREQ and RREP packet details for figure 3

	Source address	Destination sequence number	Original IP	Destination IP	HOP count
RQ1	S	16	S	D	1
RQ2	B	16	S	D	2
RQ3	C	16	S	D	3
RQ4	A	16	S	D	2
RP1	D	18	S	D	1
RP2	A	18	S	D	2

A malicious node can perform sequence number attack on AODV after receiving RREQ from the source node. It answers with a forged RREP packet containing incremented destination sequence number and lower hop count information to lure the source node to establish path through itself [10]. Assume the node A turning into a malicious node M in this scenario, as shown in Fig. 4a (assume Table 3 for Fig. 4). The malicious node M does not re-transmit the route request and sends a fictitious RP1 with higher sequence number and hop count. As a result, when S receives reply from node M, it prefers the reply sent by M as it assumes it as having a fresher route. Hence, a forged route is established through node M, which forwards data packets and drops them for the remaining time, as shown in Fig. 4b. Whether, the malicious node behavior is started during the route discovery phase to perform packet forwarding misbehavior during the data transmission phase. The success of this attack importantly depends upon destination sequence number and hop count fields in the sent route reply along with the opponent's position in the MANET.



(a) Route discovery phase (b) Data transmission phase

Fig 4: Route discovery and data transmission in AODV in the presence of a misbehavior node

TABLE 3: RREQ and RREP packet details for Fig 4

	Source address	Destination sequence number	Original IP	Destination IP	HOP count
RQ1	S	16	S	D	1
RQ2	B	16	S	D	2
RQ3	C	16	S	D	3
RP1	M	22	S	D	1
RP2	D	18	S	D	1
RP3	C	18	S	D	2
RP4	B	18	S	D	3

V. Linear regression

In Mobile Ad-hoc Network (MANET), Most of the conventional routing protocols use the path until a link breaks or failures. During the path reconstruction, packets may be lost which can cause extraordinary packet delivery ratio and throughput degradation. However, the prediction of link failures was not assumed which may reduce the network performance. A linear regression model is applied on the Received Signal Strength (RSS) of each node for forecasting the link failure time. Once the link failure time is forecast, a warning is transmitted to the source node if the link is soon-to-be-broken or failure. Then, the source node can recreate the new route before the links failure time.

The source will establish a new path discovery or utilizes another possible path from caches. Different mechanisms have been developed to manage the link failure issues in MANET, mostly by keeping more backup path to be utilizes when path failure happens. But, the chances of utilizing the backup paths are very low. Therefore, the link failure prediction is used which allows restoration of the active path before the current active path is not available. This will help to shorten the data

packet loss and improve the network performance. A linear regression model is applied on the received signal power strength for forecasting the link failure time and transfers a warning to the source node if the link is soon-to-be broken. Thus, the link failure is forecasted in earlier and prohibits the packet loss which improves the packet delivery ratio and routing performance.

VI. Proposed Solution to mitigate effect of sequence number attack

In this section, we suggest a proactive approach to label sequence number attacks which uses linear regression technique to forecast the destination sequence number of the received RREP. As shown in Fig. 5, when a node receives RREP, it forecasts the value of the destination sequence number using linear regression [32].

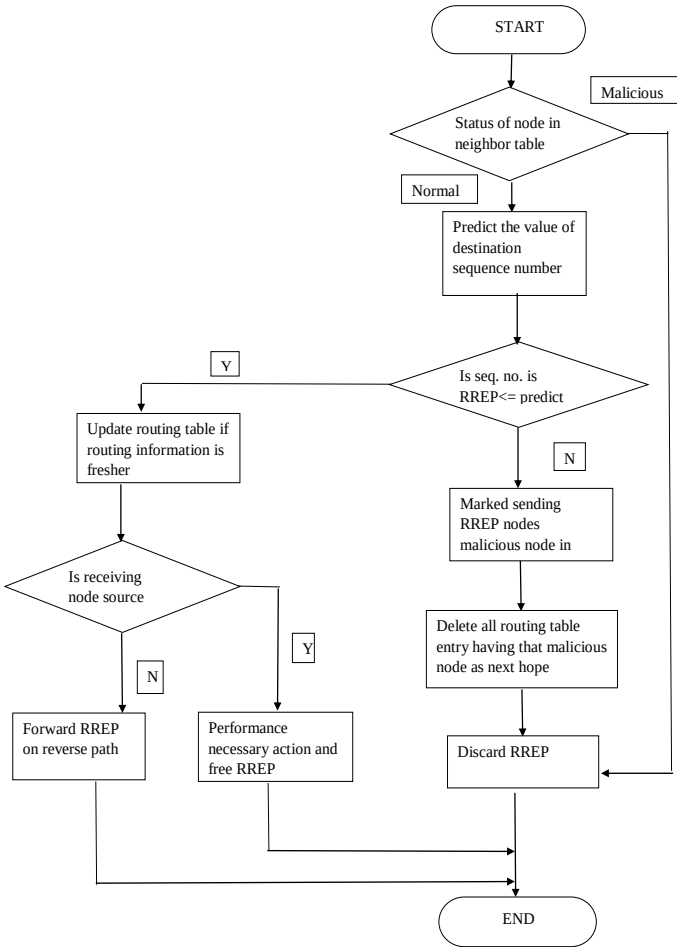


Fig 5: Proposed Approach

By the use of sequence number and historical data of time, predicted value is then compared with the actual value of the destination sequence number that is received from the RREP. If the RREP destination sequence number more than the predicted value then the node sending RREP is marked as a malicious node. In addition, the routing table entry is removed from the table whose next hop is found as malicious node. However, if the RREP destination sequence number is less than the predicted value, then normal protocol operations are performed and, time of receipt of RREP and destination sequence number value are saved in a data structure containing past entries. The normal RREP is then forwarded on the reverse route towards the source node. Thus, with the help of this proactive scheme, it attempts to identify that malicious nodes in the network during the route discovery process in order to improve the packet delivery rate.

VII. Conclusion

Security in MANETs has become one of the most important research areas during these days. There have been many secure routing schemes that are proposed by different researchers. It is to be noted that sometimes comparison of these approaches inappropriate because of different approaches have been developed for different conditions and applications. Every approach has its own constraints. We propose a proactive predictive approach for AODV protocol which is based on the principle of linear regression. This approach aims to recognize adversaries during route discovery phase to improve Quality of Services in MANETs, especially for those applications for which packet delivery rate is a pivotal parameter. There is still a prominent scope for advance research in the field of ad-hoc networks and its variants to improve their performance.

REFERENCES

1. Li W, Joshi A (2008) Security issues in mobile ad hoc networks-a survey. Department of Computer Science and Electrical Engineering, University of Maryland, Baltimore County, pp 1–23.
2. Mittal, Poonam, Sanjay Batra, and C. K. Nagpal. "Implementation of a novel protocol for Coordination of nodes in Manet." International Journal of Computer Networks and Applications 2, no. 2 (2015): 99-105.
3. Pathan ASK (ed) (2016) Security of self-organizing networks: MANET, WSN, WMN, VANET. CRC Press, Boca Raton.
4. Kannhavong B, Nakayama H, Nemoto Y, Kato N, Jamalipour A (2007) A survey of routing attacks in mobile ad hoc networks.IEEE WirelCommun 14(5). https://doi.org/10.1109/MWC.2007.4396947
5. Luo J, Fan M, Ye D (2008) Black hole attack prevention based on authentication mechanism. In: Communication Systems, 2008.ICCS 2008. 11th

IEEE Singapore International Conference on IEEE, pp 173–177
6. Jhaveri RH, Patel NM (2015) A sequence number-based bait detection scheme to thwart grayhole attack in mobile ad hocnetworks. WirelNetw 21(8):2781–2798
7. Jhaveri RH, Narendra MP (2017) Attack-pattern discovery based enhanced trust model for secure routing in mobile ad-hoc networks. Int J Commun Sys 30(7). https://doi.org/10.1002/dac.3148
8. Alheeti KMA, Gruebler A, Mcdonald-Maier K (2017) Using discriminant analysis to detect intrusions in external communication of self-driving vehicles. Digital CommunNetw 3(3):180–187
9. Singh O, Singh J, Singh R (2017) An intelligent intrusion detection and prevention system for safeguard mobile adhoc networks against malicious nodes. Indian J Sci Technol 10(14). https://doi.org/10.17485/ijst/2017/v10i14/110833
10. Gundluru N, Pradeep Reddy CH (2017) Soft-computing based trust management framework for group key management in MANETs. Int J IntellEng Sys10:327–336.https://doi.org/10.22266/ijies2017.0630.37
11. Dhananjay an G, Subbiah J (2016) T2AR: trust-aware ad-hocrouting protocol for MANET. Springer plus 5(1):995
12. Muthuramalingam S, Suba Nachiar T (2016) Enhancing the security for manet by identifying untrusted nodes using uncertainty rules. Indian J Sci Technol9(4). https://doi.org/10.17485/ ijst/2016/v9i4/87043
13. Babu SV, Afrose S, Vijila CKS (2016) An effective attack elimi-nation method for top-k query processing in MANETS. pp 9–12
14. Manoharan R, Sengathir J (2016) Erlang coefficient based con-ditional probabilistic model for reliable data dissemination in MANETs. J King Saud Univ – Comput Inform Sci 28(3):289–302
15. Li Wenjia, Song Houbing (2016) ART: an attack-resistant trust management scheme for securing vehicular ad hoc networks. IEEE Trans IntellTransp Syst 17(4):960–969
16. Rathnamma MV, Reddy PC (2016) A relationship-based approach for energy aware secure routing in MANETs. Int J Smart Grid Green Commun 1(1):87–101
17. Kumar Adarsh, Gopal Krishna, Aggarwal Alok (2016) Design and analysis of lightweight trust mechanism for secret data using lightweight cryptographic primitives in MANETs. IJ NetwSecur 18(1):1–18
18. Sengathir J, Manoharan R (2015) Exponential reliability coeffi-cient based reputation mechanism for isolating selfish nodes in MANETs. Egypt Inform J 16(2):231–241
19. Poongodi M, Bose S (2015) Detection and prevention system towards the truth of convergence on decision using Aumann agreement theorem. Procedia–Procedia Compute Sci 50:244–251
20. Patel AD, Chawda K (2015) Dual security against Gray hole attack in MANETs. In: Jain LC, Patnaik S, Ichalkaranje N (eds) Intelligent computing, communication and devices: proceedings of ICCD 2014, vol 2. Springer, New Delhi, pp 33–37
21. Sengathir J, Manoharan R (2015) A futuristic trust coefficient-based semi- Markov prediction model for mitigating selfish nodes in MANETs. EURASIP J WirelCommunNetw 2015:158. https://doi.org/10.1186/s13638-015-0384-4
22. Priyadarshini MR, Prasanna S, Balaji N (2014) Energy and mobility-based group key management in mobile ad hoc net-works. In: 2014 International Conference on Recent Trends in Information Technology, Chennai. pp 1–7. https://doi.org/10.1109/ICRTIT.2014.6996130
23. Wang Xiao, Yang Jing, Li Zetao, Li Handong (2014) The energy-efficient group key management protocol for strategic mobile scenario of MANETs. EURASIP J WirelCommunNetw 2014(1):161
24. Kamaraj N, Senthil Kumar C, Manikandan T, SebastinAlbina C, Shitharth S (2014) Modified TSR protocol to support trust in MANET using fuzzy. Int J Innov Res Sci Eng Technol 2551–2555
25. Introduction to linear regression Olinestatebook.com (2018) http://onlinestatebook.com/2/regression/inro.html.Accessed 2Jan 2018