Secure routing in mobile Ad hoc networks: A predictive approach

Aneri M. Desai
Dept. of Information technology
SVM Institute of technology
Bharuch, India
aneridesai2810@gmail.com

Rutvij H. Jhaveri
Dept. of Computer Engineering
SVM Institute of technology
Bharuch, India
rhj_svmit@yahoo.com

ABSTRACT

In recent years, wireless technologies have gained enormous popularity and used vastly in a variety of applications. Mobile Ad-hoc Networks (MANET) are temporary networks which are built for specific purposes. They do not require any pre-established infrastructure. The dynamic nature of these networks makes them more utilizable in ubiquitous computing. Due to their dynamic nature, these autonomous systems of wireless mobile nodes can be set up anywhere and anytime. However, due to high mobility, absence of central authority and open media nature, MANETs are more vulnerable to various security threats. As a result, security issues are higher in these networks as compared to the traditional networks. Ad-hoc networks are highly susceptible to various types of attackers. Out of a number of security threats, sequence number attacks are hazardous attacks which greatly diminish the performance of the network in different scenarios. Sequence number attacks suck some or all data packets and discard them. Furthermore, in this types of attacks nodes behave as a genuine node for a certain time and later on partially or completely disrupts the network. In past few years, various researchers proposed various solutions for detecting the sequence number attacks. In this paper, we survey notable works done by various researchers to detect sequence number attacks. In this paper, we address the security issues by proposing the proactive approach such as sequence number based predictive approach which discovers misbehavior nodes during route discovery phase. This approach worked with Ad-hoc on-demand distance vector (AODV) routing protocol. Using this protocol we proposed a sequence number attack based adversary model. Along with this, we discuss the future scope for these existing schemes which may prove to be beneficial to researchers for further research in this direction.

Keywords

Mobile Ad-hoc Network, Prediction, Security, Secure Routing, Routing Attacks.

1. INTRODUCTION

Over the years, growth of mobile devices has changed the world and it has become one of the most important topics in the computer world. Wireless networks have a ubiquitous nature in which nodes are connected through wireless links. In a wireless network all nodes are connected with an interconnection method such that ubiquitous devices are not connected with wired link whenever they need to get connected with other ubiquitous devices [1].

Due to the increased mobility of the users, addressing mobility issue has become a huge problem with the fixed wired infrastructure. Over the years, wireless technology has become increasingly popular and usage of this technology has defined a new paradigrim in the networking domain. Ad-hoc network is a kind of wireless network, which gets established for a specific purpose for short duration. Unlike the traditional networks, nodes are connected in homogeneous or heterogeneous manner in this network using wireless links. An ad-hoc network does not depend on a previously established infrastructure such as routers and access points. The ad-hoc network defines terms openness, self-organized, dynamic, distributed, resource-constrained and infrastructure-less. An ad-hoc network is used for different purposes such as information sharing among the network or infrastructure-less communication. When users are not connected through a wired link and if a user wants to transfer data among multiple users, a mobile ad-hoc network can be invariably used [2].A .Mobile ad-hoc network (MANET) is a wireless network that attracted many researchers in the last decade. A MANET is a cheaper, small scale and powerful solution when infrastructure wireless networks are not feasible. MANETs have become popular and faster growing area in the field of wireless networks. A numbers of nodes in the MANET form an arbitrary topology and adopt multi-hop communication such that nodes that are within each other’s radio range can communicate directly through wireless links; whereas nodes that are far apart must rely on intermediate nodes to act as routers to relay messages [3], [4].

In the field of ad-hoc networks, security has become a key research area due to their operations in hostile environments. 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 introduce new security problems in addition to the ones already present in the infrastructure wireless networks [5]. Therefore, securing a MANET is a challenging issue which needs to be addressed by understanding possible forms of attacks and prevention mechanisms for those attacks [6].

In a network, attacks can be categorized in different types based on their characteristics [7]: active attacks involve actions such as the replication, modification, and deletion of exchanged data while passive attacks do not disrupt the operation of a protocol; they only collect the information by observing of the network.

In this paper, we review different predictive techniques which address the key issue of security in wireless ad-hoc networks. For that we review different papers on prediction technique to improve security related issues. Based on that survey, we focus on sequence number attacks which are a big threat on the network layer of MANETs. Sequence number attack is type of DoS (Denial-of-Service) attack in which misbehavior nodes are authorized by network that is misbehavior nodes entre in network because of security issues such as availability [8],[9].This type of attacks are easily entre in reactive protocol such as AODV and DSR (dynamic source routing), therefore we are focus on reactive protocol that is AODV.

In AODV routing protocol maintain routes by increasing sequence number to routes for specific destinations. Freshness of route determine by destination sequence number and based on that highest sequence number based fresher route preferable for routing or updating based decision. In AODV source node start route discovery process by broadcasting request to their neighbor nodes until that time where request packet reach to destination node [10]. For establish path malicious node not have fresher router in routing table then also malicious node create forge RREP with highest sequence number and put itself in routing path and generate forge route. Once the path establish, malicious node drops the packet for specific destination or some amount of time or randomly based on packet id and switches to normal behavior[11].This type of behavior of malicious node degrade the performance of network therefore detection and prevention of this type attacker node is important for network.

During literature survey realized that most of worked done claims to detection and prevention of this type of attackers without identify the exact operation of adversary model. To identify attackers it is important that learned the operation performed by attackers therefore adversary model is important to identify [11]. In this paper, we focus on adversary model in which randomly increment destination sequence number and hop count is also increment randomly in specified range. In this adversary, an attacker randomly drops number of packets during entire life span of network.

We propose a proactive approach such as predictive approach which is identifies malicious node in network. In this approach, receiving node calculates predict value for particular destination based on its historical data. If destination sequence number exceeds the predicted value then node marked as malicious node and remove its entry form routing table whose next hop as malicious node; otherwise it is forwarded to source node .Thus, the scheme attempts to identify malicious node in network and tries to secure the route discovery process.

The rest of the paper is organized as follows: Section II represents related work in routing security of ad-hoc networks with predictive approaches, and finally, Section III concludes the paper.

2. RELATED WORK

Security is a prime area of concern in the practical implementations of the MANETs. 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.

Sengathir et al. [12] introduced an Exponential Reliability Coefficient based Reputation Mechanism (ERCRM), in which the selfish nodes are isolated from the routing path using an exponential reliability coefficient (ExRC). Reliability of coefficient is manipulated 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 isolation is carried out. Estimation of the energy level of intermediate nodes in the routing path considers two parameters viz. the residual power and power drain rate. The scheme predicts a value using the energy level, which is based on the matrix to increase security and reliability of the network.

Alheeti et al. [13] devised intrusion detection and prediction technique for detecting denial-of-service (DoS) and blackhole attacks in vehicular ad-hoc networks (VANETs). The technique is proposed 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 predict the attack based on the observations of vehicles' behavior. Fuzzification of data is carried out for generating final results which indicate behavior of different nodes. After detecting malicious or abnormal behavior, mobility and traffic scenarios are generated.

Poongodi et al. [14] proposed a scheme which uses Truth Convergence based Aumann Agreement Theorem for detection and prevention of attacks in MANETs. It extracts the behavior of nodes and identifies its patterns. Based on that, it predicts the future attacks in the network. It uses Finding Truth Convergence based confidence value which identifies false positives and false negatives in terms of malicious behavior of the nodes. A trust value is calculated 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 target nodes in the system. Aumann Agreement theorem is used to calculate 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.

Dhananjayan et al. [15] proposed a Trust-aware Ad-hoc Routing (T2AR) protocol which calculates the trust level between the nodes in the MANET and performs a secure data transmission between nodes. It predicts a trust value based on energy, mobility, and RSSI based distance measurement. This protocol obtains the information from neighbor to report the success and failure rate of packet transmission. The trust value is estimated based on the packet sequence ID matched with log reports of the node. Hence, in the proposed work, the trust value is computed through estimation of energy, the success rate of packets delivery and mobility. The direct estimation of trust value is carried out using a Bayesian framework by observation of the nodes.

Wang et al. [16] 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 performed for security and energy efficiency in the network. For creating a group, observe the neighbor nodes and then predict the quality of the link between them. After establishing a group, second functionality is performed 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 impacts to enhance the multicast energy efficient and secret communication among roaming users.

Subbaraj et al. [17] devised an Eigen Trust based non cooperative game model which is used to observe selfish behavior of a node when it fails to send data packets in the MANET. To improve QoS in the network, a secure route is discovered based on a trust model which isolates selfish or malicious nodes in the route. This game based strategy depends on the past behavior of a node and trust level between intermediate nodes. Every node in a route maintains a trust table and based on that it predicts the new trust values and probabilities. Here Eigen trust value is predicted based on direct observation of nodes' behaviors. Based on Eigen trust value, local trust values are obtained which defines that transaction is satisfactory or unsatisfactory. Also, a fuzzy based system is used which observes the number of message updates for each node in the network.

Muthuramalingam et al. [18] proposed a scheme which is used to investigate network security by calculating trust value using direct and indirect observations. To calculate the trust value with direct observations, full probability based Bayesian interface is used while with indirect observations, neighbor hop based information is used. To calculate 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 finding the shortest route between nodes in the network.

Singh et al. [19] proposed an intrusion detection and prevention system which is used for detecting malicious nodes in MANETs. This trust-based mechanism identifies malicious nodes by behavior classifier on the basis of predefine threshold and risk factor conditions. Direct and indirect trust values are used to calculate the aggregated trust value. A risk factor is calculated using these two trust components.

Gundluru et al. [20] proposed a Trust based Framework for Group Key Management which is intended to consume less computing power and to secure MANETs against internal as well as external attacks. It saves 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 calculation, a fuzzy concept is adopted in order to get the degree of trustworthiness instead of binary classification. It uses clustering approach in which a cluster leader is selected for each cluster. Cluster leader periodically predicts 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.

Babu et al. [21] proposed a scheme that is used to identify data replacement attack and false notification attack in MANETs. The proposed method detects these attacks by using a score value in top k query processing. It broadcasts false notification information to all other nodes to disseminate information about malicious nodes in the network. A node sends its own predicted score value along with a path value to decide a particular path to send data.

Manoharan et al. [22] devised an Erlang Coefficient based Conditional Probabilistic Model for isolating selfish nodes through the manipulation of Conditional Probabilistic Coefficient (CPC) factor. This factor acts as reputation factor for estimating negative impact produced by selfish nodes. In this model, three steps are performed. In the first step, the detection of selfish node is carried out based on a genius factor. Genius factor is predicted by neighbor nodes using packet forwarding and receiving rates. In the second step, an estimation of a non-cooperative factor is carried out. This factor depends on the number of selfish nodes present in a routing path between source and destination nodes. Selfish nodes are identified by the above Genius factor. In the third step, determination of CPC is performed based on Erlang Distribution. This approach predicts the failure rate of cooperative nodes. This approach depends on two independent exponential random variables. Based on these three steps, it isolates selfish nodes in the routing path.

Ahmed et al. [23] proposed a Flooding Factor based Trust Management Framework which is used for identifying malicious nodes in MANETs. A modified route discovery algorithm is also used for efficient and secure data forwarding through the route. Moreover, Experimental Grey Wolf algorithm is used for validating network nodes. Using this algorithm, nodes with key values are found and node details are verified. This searching of individual nodes is helpful to identify attacks in the network. A True Flooding algorithm is used to define the highest probability of link failure due to the behaviors of attacker nodes and normal nodes. Route discovery algorithm uses key assignment, identifies.

Li et al. [24] proposed an Attack-Resistant Trust Management Scheme which is used to detect malicious nodes and to evaluate trustworthiness of data in VANETs. In this scheme, data trust is predicted on the basis of data sensed from multiple vehicles. Trust is assessed 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. [25] proposed a scheme to provide trust based secure routing in MANETs. Four types of trust are calculated and based on that energy of the nodes is calculated. In the first type, initial trust is considered which gives same priory to all the nodes by giving them initial trust value. In the second type, behavioral trust is calculated based on behaviors of the nodes. In the third type, neighbor trust is calculated based on direct and indirect trust components. Finally, based on all these three types, a final trust value is calculated.

Patel et al. [26] proposed a scheme, used for providng securtiy 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 packe accept otherwise reject that packet. After that in data transmission phase each node maintain threshold value . If threshold value of that node beat to the node sequence number than discard that reply packet . otherwise check that receving 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 calcultation of threshold value done on base of routing table sequence number, number of data packet send from node and number of data packet recevie from node.

Priyadharshini et al. [27] proposed 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 formulated by metrics of received power and distance between nodes. Mobility prediction is carried out by observing different patterns of connectivity. Next value of time series is predicted 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.

Sengathir et al. [28] proposed a Futuristic Trust Coefficient based Semi Markov Prediction Model to investigate and quantify the impact of selfish nodes in MANETs. The Semi Markov Prediction model defines the lower and upper bound of network survivability. It identifies and isolates the selfish nodes from the routing path based on a futuristic trust coefficient. In this model, first stochastic properties of mobile nodes are estimated. For this estimation, it uses input parameters of source and destination nodes and then, it estimates 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 futuristic behavior of a node is estimated and, based on that, isolation of a selfish node is carried out.

Senthilkumar et al. [29] proposed a scheme which is used to identify dishonest nodes in MANETs. Trust value of a node is predicted 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 divided into two parts: subjective evaluation model and trusted routing model. In the subjective evaluation model, a trust value is calculated based on trustworthiness of nodes. Based on the analytic hierarchy process, decision about the nodes and their future behaviors are predicted. This decision and prediction are used to isolate untrustworthy nodes and to establish a secure route towards the destination.

Kumar et al. [30] proposed a scheme for identifying the resource constrained mobile nodes in MANETs. In this scheme, a centralized environment is established using groups and subgroups. Probability analysis of distance bounding protocol shows 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 provide an efficient and secure route. For lightweight grouping, it performs collection of node information and propagation of the information. Once the subgroup is created, protection from various attacks and relationship maintenance are carried out by a trust model. The trust management includes trust generation, trust propagation, trust accumulation, trust prediction and trust application.

Xia et al. [31] 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. Based 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 calculate 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 predicate 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 based on data and control packet of node.

3. Proposed Methodology

In this section, we propose a proactive approach which is predictive approach, which uses linear regression technique using the destination sequence number of the received RREP and that of the routing table. This action is performed by receiving RREP node .In this approach node first check the status of node in neighbor table, whether node status as malicious node then node discards its RREP and either node status as normal node in neighbor table then perform prediction using linear regression techniques.

Using linear regression techniques [32] it first predicts destination sequence number of node. In this approach, receiving node calculates predict value for particular destination based on its historical data. In routing table we collect historical data for every destination. In historical data we collect sequence number of destination at particular time. Using this historical data with linear regression its predict sequence number for destination at current time. If destination sequence number exceeds the predicted value then node marked as malicious node and remove its entry form routing table whose next hop as malicious node; otherwise it is forwarded to source node .Thus, the scheme attempts to identify malicious node in network and tries to secure the route discovery process.

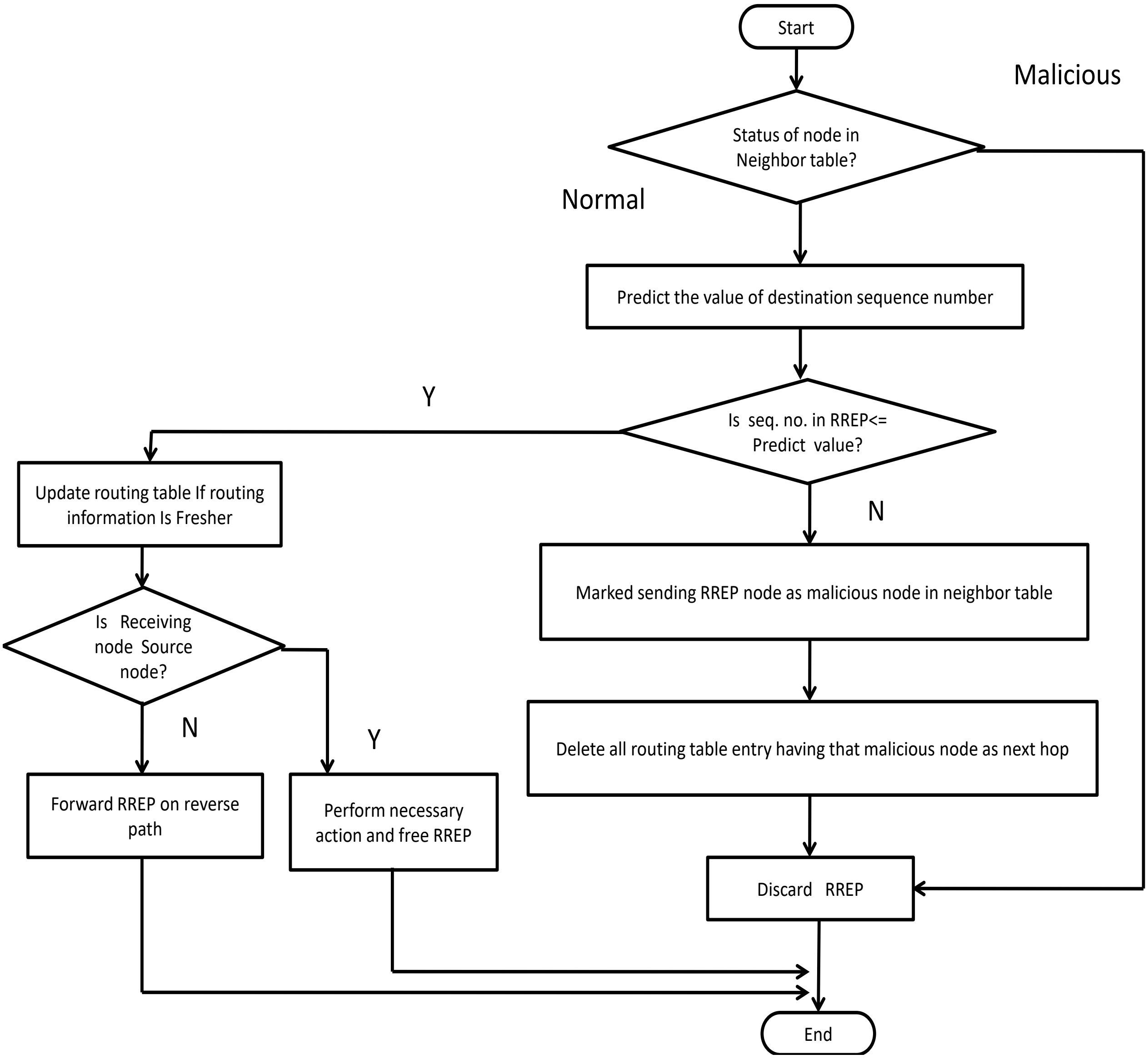
Start
Malicious
Status of node in Neighbor table?
Normal
Predict the value of destination sequence number
Y
Is seq. no. in RREP<= Predict value?
N
Update routing table If routing information Is Fresher
Marked sending RREP node as malicious node in neighbor table
Is Receiving node Source node?
N
Y
Delete all routing table entry having that malicious node as next hop
Forward RREP on reverse path
Perform necessary action and free RREP
Discard RREP
End

Figure 1: Action Performed by receiving RREP node.

4. Adversary Model

In this adversary mode, misbehavior node receive an RREQ, it cannot propagate RREQ towards the destination node it directly sends RREP towards the source node. Source node receives number of RREQ from other path therefore misbehavior node establish path towards its RREQ it sends RREP with highest sequence number. To attack source node and to establish path through itself misbehavior node filled RREP with randomly increment value of destination sequence number and hop count value is also randomly increment within specified range. Paths establish through misbehavior node therefore misbehavior node drops random number of packet during entire life span of network.

4.1 Sequence Number Attack in AODV-based MANETs

As shown in figure 2(a), source node S wants to communicate with a destination node D. It broadcast route request RQ1 with last known destination sequence number 15, which is received by the neighbor nodes 1 and 3 in communication range. The receive packets are rebroadcast again by receiving node 1 and 3 RQ2 and RQ4 to its neighbor nodes. The receiving node rebroadcasting that packet until node having destination itself to receive it. Destination node D receive first route request RQ4 from node 3. Meanwhile node 2 has also send route request packet RQ3 to destination node D but destination node receive request first from node 3 so it discard RQ3 from node 2 therefore that forward RP1 on reverse path to source node S with sequence number value 20. This reply packet is forwarded towards source node through intermediate node 3. AS a reply from D to source node S, Select the route S-3-D to transfer data packets as shown in figure 2(b).

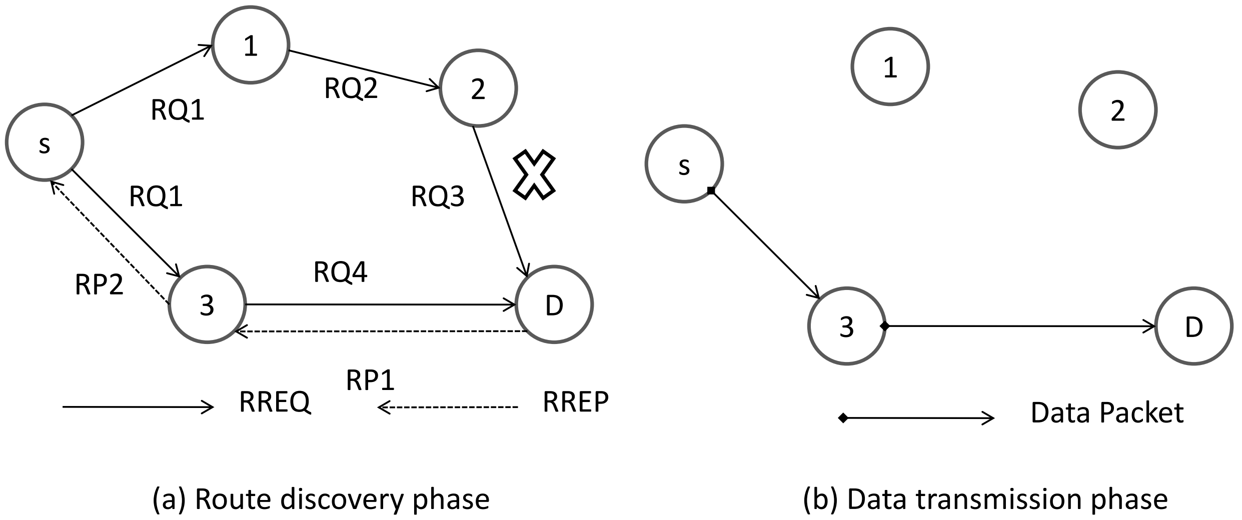

Figure 2: Route discovery and data transmission in AODV

Table 1: RREQ and RREP packet detail for fig 2.

	RQ1	RQ2	RQ3	RQ4	RP1	RP2
Source IP	S	1	2	3	D	3
Dest Seq Number	15	15	15	15	20	20
Origin IP	S	S	S	S	S	S
Destination IP	D	D	D	D	D	D
Hop Count	1	2	3	2	1	2

A malicious node launches Sequence number attack on AODV after receiving RREQ from the source. It responds with a bogus RREP packet containing randomly increment destination sequence number and hop count information to attract the source to establish path through itself. After getting succeeded during the route discovery phase, it performs packet forwarding misbehavior during the data transmission phase.

Consider the node 3 turning into a malicious node M in the scenario, as shown in Figure. 3(a) .The malicious node M does not re-broadcast the route request and sends a forged RP1 with random sequence number and hop count. As a result, when S receives replies from node M, it prefers the one sent by M. Hence, a bogus route is established through node M, which forwards data packets and drops them for the remaining time, as shown in Figure. 3(b).

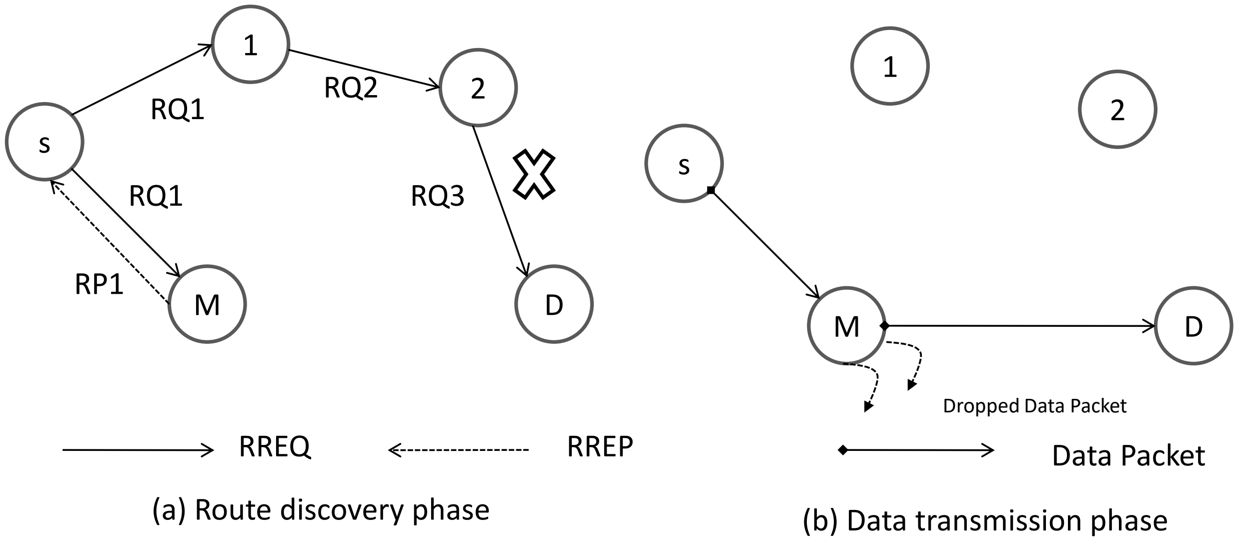

Figure 3: Route discovery and data transmission in AODV in the presence of a misbehavior node

Table 2: RREQ and RREP packet detail for fig 3.

	RQ1	RQ2	RQ3	RQ4	RP1	RP2
Source IP	S	1	2	3	D	3
Dest Seq Number	15	15	15	15	25	25
Origin IP	S	S	S	S	S	S
Destination IP	D	D	D	D	D	D
Hop Count	1	2	3	2	2	3

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 prominently depends upon destination sequence number and hop count fields in the sent route reply along with the adversary's position in the MANET.

5. CONCLUSIONS

Security in MANETs has become one of the fastest growing research areas in recent years. There have been various schemes proposed by various researchers which address security of these dynamic networks. The aim behind conducting this work is to provide a detailed survey of these approaches in distinct types of ad-hoc networks. It is to be noted that comparison of different approaches with each other is not practical as different approaches have been developed for different situations and applications. In spite of this, each of these approaches has its own limitations. In this paper, we proposed a predictive approach for aodv protocol which is based on destination sequence number. This approach identifies sequence number attack during route discovery phase and propagates information about malicious node to other node in network. We conclude that still there is a huge room for further research in the field of wireless ad-hoc networks and its variants to enhance their performance by incorporating efficient energy conservation schemes, authentication and key distribution mechanisms, secure routing solutions and performance optimization techniques.

6. REFERENCES

[1] W. Li and A. Joshi, "Security Issues in Mobile Ad Hoc Networks-A Survey," *Dep. Comput. Sci. Electr. …*, pp. 1–23, 2008.

[2] P. P. Patel and R. H. Jhaveri, "Various schemes to detect selfishness in wireless ad-hoc networks: A survey," *Proc.*

2015 Int. Conf. Green Comput. Internet Things, ICGCIoT 2015, pp. 881–886, 2016.

[3] A.-S. K. Pathan, “Security of self-organizing networks: MANET, WSN, WMN, VANET.” p. 638, 2010.

[4] B. Kannhavong, H. Nakayama, Y. Nemoto, N. Kato, and A. Jamalipour, “A survey of routing attacks in mobile ad hoc networks,” *IEEE Wirel. Commun.*, vol. 14, no. 5, pp. 85–91, 2007.

[5] J. Luo, M. Fan, and D. Ye, “Black hole attack prevention based on authentication mechanism,” *2008 11th IEEE Singapore Int. Conf. Commun. Syst. ICCS 2008*, pp. 173–177, 2008.

[6] I. Chlamtac, M. Conti, and J. Liu, “Mobile ad hoc networking: imperatives and challenges,” *Ad Hoc Networks*, pp. 153–158, 2003.

[7] P. Paper, “IEI "’,” 2011.

[8] M. Zolfaghari, M. Sadeghzadeh, R. Frouzande, and A. Emami, “Methods for Detection and Removal of Grayhole Attack in Mobile Adhoc Network (MANET),” vol. 5, pp. 15–19, 2016.

[9] V. Dwivedi and S. Ahmad, “Detection and Prevention Methods of Black Hole & Gray Hole Attacks in MANET – A Critical Survey,” pp. 187–192, 2016.

[10] R. H. Jhaveri and N. M. Patel, “A sequence number based bait detection scheme to thwart grayhole attack in mobile ad hoc networks,” *Wirel. Networks*, vol. 21, no. 8, pp. 2781–2798, 2015.

[11] R. H. Jhaveri and N. M. Patel, “Attack-pattern discovery based enhanced trust model for secure routing in mobile ad-hoc networks,” 2016.

[12] J. Sengathir and R. Manoharan, “Exponential Reliability Coefficient based Reputation Mechanism for isolating selfish nodes in MANETs,” pp. 231–241, 2015.

[13] K. M. A. Alheeti, A. Gruebler, K. M. A. Alheeti, A. Gruebler, and K. Mcdonald-maier, “Author ’ s Accepted Manuscript Using Discriminant Analysis to Detect Intrusions in External Communication of Self-Driving Vehicles Reference : To appear in : Digital Communications and Networks Using Discriminant Analysis to Detect Intrusions in External Communication of Self-Driving Vehicles,” *Digit. Commun. Networks*, 2017.

[14] M. Poongodi and S. Bose, “Detection and Prevention system towards the truth of convergence on decision using Aumann agreement theorem,” *Procedia - Procedia Comput. Sci.*, vol. 50, pp. 244–251, 2015.

[15] G. Dhananjayan and J. Subbiah, “T2AR : trust - aware ad - hoc routing protocol for MANET,” *Springerplus*, 2016.

[16] X. Wang, J. Yang, Z. Li, and H. Li, “The energy-efficient group key management protocol for strategic mobile scenario of MANETs,” pp. 1–22, 2014.

[17] S. Subbaraj and P. Savarimuthu, “EigenTrust-based non-cooperative game model assisting ACO look-ahead secure routing against selfishness,” 2014.

[18] S. Muthuramalingam and T. S. Nachiar, “Enhancing the Security for Manet by Identifying Untrusted Nodes using Uncertainity Rules,” vol. 9, no. January, 2016.

[19] O. Singh, J. Singh, and R. Singh, “An Intelligent Intrusion Detection and Prevention System for Safeguard Mobile Adhoc Networks against Malicious Nodes,” vol. 10, no. April, pp. 1–12, 2017.

[20] N. Gundluru, “Soft-Computing Based Trust Management Framework for Group Key Management in MANETs,” vol. 10, no. 3, pp. 327–336, 2017.

[21] S. V. Babu, S. Afrose, and C. K. S. Vijila, “AN EFFECTIVE ATTACK ELIMINATION METHOD FOR TOP-K QUERY PROCESSING IN MANETS,” no. December, pp. 9–12, 2016.

[22] R. Manoharan and J. Sengathir, “Erlang coefficient based conditional probabilistic model for reliable data dissemination in MANETs,” *J. King Saud Univ. - Comput. Inf. Sci.*, vol. 28, no. 3, pp. 289–302, 2016.

[23] M. N. Ahmed, A. H. Abdullah, H. Chizari, and O. Kaiwartya, “F3TM : Flooding Factor based Trust Management Framework for secure data transmission in MANETs,” *J. KING SAUD Univ. - Comput. Inf. Sci.*, 2016.

[24] W. Li, H. Song, and S. Member, “ART : An Attack-Resistant Trust Management Scheme for Securing Vehicular Ad Hoc Networks,” vol. 1, no. c, pp. 1–10, 2015.

[25] M. V Rathnamma and P. C. Reddy, “A relationship-based approach for energy aware secure routing in MANETs,” vol. 1, no. 1, pp. 87–101, 2016.

[26] A. D. Patel and K. Chawda, “Dual Security Against Grayhole Attack in MANETs,” in *Intelligent Computing, Communication and Devices: Proceedings of ICCD 2014, Volume 2*, L. C. Jain, S. Patnaik, and N. Ichalkaranje, Eds. New Delhi: Springer India, 2015, pp. 33–37.

[27] M. R. Priyadharshini, S. Prasanna, and N. Balaji, “Energy and Mobility Based Group Key Management in Mobile Ad Hoc Networks,” 2014.

[28] J. Sengathir and R. Manoharan, “A futuristic trust coefficient-based semi- Markov prediction model for mitigating selfish nodes in MANETs,” *EURASIP J. Wirel. Commun. Netw.*, 2015.

[29] C. Senthilkumar, T. Manikandan, C. Sebastinalbina, S. Shitharth, and N. Kamaraj, “Modified TSR Protocol to Support Trust in MANET Using Fuzzy,” vol. 3, no. 3, 2014.

[30] A. Kumar, K. Gopal, and A. Aggarwal, “Design and Analysis of Lightweight Trust Mechanism for Secret Data using Lightweight Cryptographic Primitives in MANETs,” vol. 18, no. 1, pp. 1–18, 2016.

[31] H. Xia, Z. Jia, X. Li, L. Ju, and E. H. Sha, “Ad Hoc Networks Trust prediction and trust-based source routing in mobile ad hoc networks,” *Ad Hoc Networks*, vol. 11, no. 7, pp. 2096–2114, 2013.

[32] “Introduction to Linear Regression “, *Olinestatebook.com*, 2018. [Online]. Available: http://onlinestatebook.com/2/regression/inro.html. [Accessed: 2-Jan-2018].

Table 1. Literature Review

Title	Author , Publisher and year	Methodology	Objective	Performance Metrics	Future Scope	Simulator	Proactive	Reactive
Exponential reliability coefficient based reputation mechanism for isolating selfish node in MANETS	J.sengathir et al. .Elsevier (2015) [12]	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 behaviour of mobile nodes.	NS-2	Yes	Yes
Using Discriminate Analysis to Detect Intrusions in External Communication of Self-Driving Vehicles	Khattab M Ali Alheeti et al.Elsevier (2015 [13]	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	NS-2	Yes	No
Detection and Prevention System towards the Truth of Convergence on decision using Aumann agreement theorem	M.Poongodi et al .Elsevier (2015) [14]	Truth Convergence based Aumann agreement Theorem	Detection and prevention of dos attack by identify the behaviour of a node .	Detection range, Packet delivery Ration	Trust estimation with bound of confidence in a multi-relay access network with heterogeneous environment	NS-2	No	Yes
T2AR: trust - aware ad-hoc routing protocol for MANET	Gayathri Dhananjayan et et al.Springer Plus(2016) [15]	Neighbour 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..	NS-2	No	Yes
The energy - efficient group key management protocol for strategic mobile scenario of MANETs	Xiao Wang et al. Springer (2014) [16]	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.	MATLAB ,NS-2,OPNET	No	Yes
Eigen Trust - Based non-cooperative game model assisting ACO look-ahead secure routing against selfishness	Surendran Subbaraj et al. Springer (2014) [17]	Local Trust evaluation using eigen Trust, Certificate Authority election, Fuzzy -based trust system.	Identifying selfish behaviour by finding trusted valid route.	Packet delivery ratio, Throughput, Routing overhead	Evaluation against mixture of selfish and malicious nodes, and further developing trusted secured routing techniques	NS-2	No	Yes
Enhancing the Security for MANETs by identifying untrusted Nodes using	S. Muthuramalingam et al. INDJST (2016) [18]	Bayesian interface, Dempster - shaftertheory observation Scheme, The Dijkstra's algorithm	Isolate the misbehaving nodes from the routing path by predicting	Packet delivery ratio, packet delay, throughput	Devising trust based method with classification.	NS-2	No	Yes

Uncertainty Rules.			trust between nodes.					
An Intelligent Intrusion Detection and Prevention System for Safeguard Mobile Adhoc Networks Against Malicious Nodes	Opinder Singh et al. INDIST (2017) [19]	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.	NS-2.3	No	Yes
Soft-computing Based Trust Management Framework for Group Key Management in MANETs	Nagaraja Gundluru et al. INASS (2017) [20]	Group Key management, Trust management Framework(TMF),Game theory and Fuzzy logic.	Isolating internal as well as external using a 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 defence mechanisms for attacks such as bad -mouthing, ballot-stuffing, and collusion	NS-2	Yes	Yes
An effective Attack elimination method for Top -K Query processing in MANETs	S.Venkatesh Babu et al. Elysium journal of engineering research & management(2016) [21]	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.	NS-2	Yes	Yes
Eralang coefficient based conditional probabilistic model for reliable data dissemination in MANETs	R.Manoharan al. ELSEVIER (2015) [22]	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	NS-2	No	Yes
F3TM:Flooding Factor based Trust Management Framework for Secure data transmission in MANETs	Malik N.Ahmed et al. ELSEVIER (2016) [23]	Key Assignment Algorithm (KAA), new Experimental Grey Wolf, True flooding algorithm.	Efficient and secure establishment of route between souce and destination.	Average delay , overhead ,packet delivery ratio, throughput	Using a query based or group based system to find a secure route	NS-2	No	Yes
ART:An Attack-Resistant Trust Management Scheme for Securing Vehicular Ad hoc Networks.	Wenjia Liet al. IEEE (2015) [24]	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 system for route discovery.	GloMoSim 2.03	No	Yes
A relationship -based approach for energy aware secure routing in MANETs	M.V. Rathnamma et al. Inderscience (2016) [25]	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.	network simulator	No	Yes
Dual Security Against Grayhole	Patel et al. Springer (2015) [26]	Dual security based approach.	Detecting and identifying gray hole	Packet drop ratio	Perform predictive approach using	Ns2	Yes	Yes

Attack in MANETs			attack in MANETs.		other techniques.			
Energy and Mobility Based Group Key Management in Mobile Ad Hoc Networks	M.Ramya Priyadharshini et al.IEEE (2014) [27]	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	NS2	No	Yes
A Futuristic trust coefficient-based semi-markov prediction model for mitigating selfish node in MANETs	Janakiraman sengathir et al. Springer (2015) [28]	Futuristic trust coefficient -based semi-Markov prediction model , Validation and network survivability analysis of FTCSPM model	Investigating and quantifying the impact of selfish behaviour 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.	NS2	No	Yes
Modified TSR protocol to Support trust in MANET Using Fuzzy	C.Senthilkumar et al. ICIET(2014) [29]	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	NS2	No	Yes
Design and Analysis of Light Weight Trust Mechanism for Secret Data using Lightweight Cryptographic Primitives in MANETs	Adarsh Kumar et al. IJNS(2016) [30]	Lightweight Identification, lightweight grouping, lightweight trust Based distance bounding and authentication.	Predicting MANETs against the mafia Fraud, distance fraud, terrorist fraud, and distance hijacking attack	Delivery ratio, goodput , energy consumption, jitter	Using Fuzzy method to predict trust value.	NS2	No	Yes
Ad Hoc Networks Trust prediction and trust-based source routing in mobile ad hoc networks	H.Xia et. al. ELSEVIER (2013) [31]	Trust based source routing using fuzzy based prediction.	Identifying and isolating the misbehaviour using fuzzy based prediction system	Packet delivery ratio, network throughput	Determination optimal route can be based on quality of service, load and delay.	NS2	No	Yes