A novel machine learning-based attacker detection system to secure location aided routing in MANETs

R. Suma*

VTU,
Belgaum, Karnataka 590018, India
and
Department of MCA,
SSIT,
Tumkur, Karnataka 572105, India
Email: sumaraviram@gmail.com
*Corresponding author

B.G. Premasudha

Department of MCA,
SIT,
Tumkur, Karnataka 572103, India
Email: bgpremasudha@gmail.com

V. Ravi Ram

VTU,
Belgaum, Karnataka 590018, India
and
Department of MCA, SSIT,
Tumkur, Karnataka 572105, India
Email: raviramv@gmail.com

Abstract: The proposed work deals with the improvisation of the performance of location-based routing in mobile ad hoc network (MANET). A machine learning-based attacker detection (MLAD) algorithm that uses multipath routing is proposed to facilitate efficient routing even in the presence of attackers. The proposed algorithm adopts the location aided routing (LAR) to optimise the search process and to reduce the search area for new routes in MANETs. Learning automata (LA) is implemented to optimise the path selection and to reduce overhead in the network. Extended identity-base cryptography (EIBC) is used for efficient key management in providing system security. The proposed system implements privacy preserving communication system (PPCS) for maintaining privacy in end-to-end communication. This method decouples the location information from the node's identifier and abstracts the communication happening among nodes. The simulation results of the proposed method reveal its reliability and strength in securing LAR in MANETs.

Keywords: mobile ad hoc network; MANET; learning automata; optimisation; routing; fault tolerance; identity-based cryptography; key management; privacy preservation; attacker detection; location aided routing.

Reference to this paper should be made as follows: Suma, R., Premasudha, B.G. and Ravi Ram, V. (2020) 'A novel machine learning-based attacker detection system to secure location aided routing in MANETs', *Int. J. Networking and Virtual Organisations*, Vol. 22, No. 1, pp.17–41.

Biographical notes: R. Suma received her BSc (Computer Science) and Master's in Computer Applications from the Bangalore University, Karnataka, India. She is pursuing her PhD in Computer Science and Engineering from the Visvesvaraya Technological University, Karnataka, India. She has 18 years of teaching experience in Computer Science. She is currently working as an Associate Professor in the Department of Master of Computer Applications from the Sri Siddhartha Institute of Technology, Karnataka, India. Her research interests include routing and security in MANETs and VANETs.

B.G. Premasudha received her BE (Electronics) and MCA from the Bangalore University, Karnataka, India, MTech (CSE) from the JNTU, Telangana, India and PhD from the Dr. M.G.R. Educational and Research Institute, Tamil Nadu, India. At present, she is working as a Professor in the Department of Master of Computer Applications, Siddaganga Institute of Technology, Tumkur, Karnataka, India. She has 27 years of teaching experience in the area of computer science. She had published several journal articles and conference papers at national and international levels. She has several funded projects from various funding agencies and is currently providing research guidance to six PhD Scholars under Visvesvaraya Technological University, Karnataka, India. Her areas of interest include spatial analysis, location-based services, mobile computing, MANETs, VANETs and sensor networks.

V. Ravi Ram received his BSc (Applied Sciences) with Computer Science specialisation from the Andhra University, Andhra Pradesh, India and Master's in Computer Applications from the Visvesvaraya Technological University, Karnataka, India in 1998 and 2001 respectively. He is pursuing his PhD in Computer Science and Engineering from the Visvesvaraya Technological University, Karnataka, India. He has 16 years of teaching experience in computer science. He is currently working as an Associate Professor in the Department of Master of Computer Applications from the Sri Siddhartha Institute of Technology, Karnataka, India. His research interests include routing and security in MANETs and VANETs.

1 Introduction

Mobile ad hoc network (MANET) is made up of wireless mobile hosts which are not physically connected to each other and works in a virtual infrastructure. The communication in MANETs between hosts happens in multiple hops through intermediate nodes (Corson et al., 1996). Due to high mobility nature of hosts, it is difficult to maintain or find routes in MANETs. Many researchers have proposed methods that work on various routing challenges in MANETs (Corson and Macker, 1998; Jiang et al., 1998; Johnson et al., 1998; Ko and Vaidya, 1998; Krishna et al., 1995). As the mobility of nodes in MANETs is very rapid, it is optimal to discover routes only when there is a demand for it. All reactive routing protocols perform route discovery on demand and eliminate the overhead in maintaining unwanted and obsolete routes, hence they suit well for MANETs. Thus, a reactive routing protocol – location aided routing

(LAR) (Ko and Vaidya, 2000) is used in our system. This routing protocol uses the location information obtained from global positioning system (GPS) to identify the requested and expected zones in the network (Ko and Vaidya, 2000). The request zone includes both the sender and receiver in a rectangular area. Thus a reduction in the search area brings in a greater reduction in the routing overhead.

An extensive literature review on the existing machine learning-based attacker detection (MLAD) schemes is presented in Section 2 of this paper. Our work implements learning automata (LA) to optimise the path selection and to reduce overhead in the network. The LA algorithm is introduced with LAR using Steiner tree. The link stability is taken into consideration to increase the performance of MANETs. As described by Joydipa and Vinodha (2013), weights are assigned to the links and Steiner tree is formed with the nodes that are less mobile. Section 3 of this paper describes the LAR scheme, LA and its environment.

The proposed MLAD algorithm has an automaton stationed with each node. This algorithm reduces the flooding by diverting the population on an optimal path depending upon the goodness value of the path. Based on this goodness value, a reward-penalty scheme that updates the edge probability is employed. Section 4 illustrates the significance of goodness value of nodes with the reward-penalty schemes and describes the proposed MLAD algorithm.

Network security solutions have long employed cryptographic architectures as a method of securing the network as well as the data. Several researchers have put in efforts to mitigate the security threats in the MANET environment using cryptographic architectures. As described by Sumalatha and Sathyanarayana (2015), public key cryptography is being used with digital certificates for user authentication. When it comes to public key encryption, the private key generator (PKG) generates the private keys and each entity keeps its private key in secret and shares its public key with all other entities. Extended identity-base cryptography (EIBC) is used for efficient key management in providing system security. In addition to the basic elements of ID-based cryptosystems, EIBC scheme uses 'pseudo random number generator (PRNG) and a series of periodic modification functions (PMFs)'. These cryptographic methods are employed to reduce eavesdropping among nodes. Section 5 describes the EIBC mechanism with encryption and signature schemes.

From the existing literature it is clearly understood that isolation of the identity of a node from its physical location preserve node privacy. In order to safeguard node privacy, a privacy preserving communication system (PPCS) is proposed. This scheme is used to encrypt and decrypt data so as to prevent hackers and their attacks. An optimal guessing strategy on attacks is implemented in our system and it is proved that the guessing strategy does not relate to the node count on the path. The results of the simulated process had practically proved the efficiency of the system with minimal impact on packet delivery. Route selection and route evaluation methods are introduced for fault tolerance routing. These methods aid in finding the probability of successful route selection and packet delivery. The proposed scheme combines the fault tolerant routing and the cluster routing methods to achieve optimal state and avoid overheads, malicious activities and broken path issues. Section 6 of this paper proposes the PPCS scheme with dynamic flow identification, random node identification and resilient packet forwarding mechanisms with security analysis. An overview of our methodology is presented in Section 7. Simulations were carried out in NS2 with four types of routing schemes in the presence of attackers. The performance of the proposed system that integrates privacy preservation, EIBC and machine learning was compared with other schemes based on the performance metrics throughput, packet delivery ratio (PDR), routing overhead, end to end delay and packet loss. The performance evaluation of our system is described in Section 8 and the simulation results of the proposed method reveal its reliability and strength. Section 9 covers the discussion on the theoretical and practical implications of the work, followed by conclusion.

2 Literature review

Wireless networks are very much prone to attacks as the communication channels are open to the intruders. The attacker detection in MANETs can be achieved through software modules that automatically monitor malicious activities in the network. While designing an attacker detection system for MANETs we need to take into account certain thoughts. The attacker detection systems for MANETs will behave differently from their wired counterparts. There are several challenges need to be addresses while designing attacker detection systems for MANETs. Sen and Clark (2008) have made a survey on the available attacker detection methods for MANETs. The conventional anomaly-based attacker detection systems that make use of predefined models to detect network anomalies. These models cannot be directly used for MANETs as the nodes experience high mobility. Due to the rapid mobility of nodes, MANETs undergo dynamic changes in their network topologies there by increasing the complexity of attacker detection process. As the nodes in MANETs are mobile, it is not possible to deploy the attacker detection system on a particular node. This clearly conveys that the attacker detection shall be distributed among the nodes. Based on this, the attacker detection systems are classified into collaborative and non-collaborative types (Sen and Clark, 2008). The non-collaborative attacker detection systems deploy agents at the node level to watch for any suspicious activities and to report the same. The biggest difficulty lies in identifying the location of agents as the nodes are mobile. Similarly, the nodes that host the attacker detection agents demand for greater bandwidth, computational power and battery power. But these resources are limited in MANETs. Increasing the attacker detection rate with limited resources becomes an NP-complete problem and several authors have proposed algorithms to give nearest solutions. There are several attacker detection architectures available for MANETS.

Zhang and Lee (2000) and Zhang et al. (2003) have proposed a collaborative and distributed attacker detection system in which the nodes are capable of independently observing their neighbouring nodes for any possible intrusions. Each attacker detection agent process is broken into several modules. The data collection module is responsible for collecting the audit traces and activity logs. The local detection module checks for any local anomalies. The local and global response modules are responsible for executing the response actions. An extra secure communication module facilitates sharing of information in a trusted manner. The authors made use of certain classifiers to predict anomalies. In this process, the detector node raises an alarm if it identifies a strange event that was not predicted earlier by the classifiers. Huang and Lee (2003) have presented a cluster-based attacker detection system to handle the constraints on MANET resources. The authors have used certain statistical inferences out of the routing tables and applied a classification decision tree algorithm. This attacker detection system is capable of identifying the source of an attack that happens within one hop range. Huang and Lee (2004) have proposed a hybrid system by integrating specification-based detection with anomaly-based detection. They have used a finite state machine that could represent the collaborative behaviour of ad hoc on demand distance vector (AODV) protocol. Sun et al. (2006) have addressed the problem of non-cooperation among the nodes by proposing an attacker detection system based on non-overlapping zone concept. In their method, the nodes are grouped into zones with certain nodes designated as gateways. By using Markov chains, a node detects any kind of abnormal activities and reports the same to its gateway node. Su (2011) had proposed a cooperative attacker detection system that is capable of sensing black hole attacks. The detector nodes broadcast messages to all other nodes to block a malicious node if it is found sending suspicious packets beyond the permissible limit. The authors Sen and Clark (2009) have proposed several ways to detect packet dropping, flooding and route disruption attacks. They were successful in detecting the three types of attacks. The authors Sen et al. (2010) have used genetic programming to maximise the attacker detection rate and minimise the energy consumption. They could address the flooding attack and the route disruption attack.

Kotov and Vasilev (2011) have proposed an adaptive routing attacker detection system for MANETs using machine learning algorithm support vector machines. The authors Joseph et al. (2007) have proved that cross layer attacker detection approach is better than using single layer approach. Shrestha et al. (2010) have proposed a cross layer attacker detection scheme using cluster data mining. Their scheme could detect DoS and sink-hole attacks. Athreya and Tague (2011) have proposed a cross layer mechanism for establishing multiple paths but they could not address security. Senthil and Kamalakkannan (2013) have proposed a cross layer approach to minimise the number of broken links. Their method could considerably reduce the packet retransmission rate. The authors Roopa and Selvakumar (2017) have proposed an intrusion detection system (IDS) for providing a layer to secure the MANETs from several attacks. The IDS could detect black hole attack and recognise multi-layer perceptron (MLP) as a secure and accurate network. Smail et al. (2017) have proposed an energy aware and stable cluster-based multipath routing (ES-CMR) scheme that safeguards the energy of the participating nodes and enhances the lifespan of the MANET. The authors have used a model that could efficiently identify energy proficient paths with steady links. Their model was proved to considerably reduce the end to end delay. Saju and Samuel (2017) have proposed a model that predicts and uses the trust level of the nodes to exchange and revoke certificates in MANETs. Their model adopts a multi-path certificate exchange technique to certify the public keys of the nodes. The certificate issuing nodes are validated by the trust prediction model before issuing the certificates. Using this technique, a source node can avoid forwarding data through malicious nodes and choose alternative paths for securely routing the information. The authors Rajkumar and Narsimha (2016) have proposed a scheme that provides security using multi path routing. In their scheme, all route request packets are signed with digital signatures. A destination node upon receiving the route request verifies the signature and caches the session key of the source node. The destination node sends the route reply packet on the same path. They have used an optimal algorithm to secure routing paths in an optimal way. The source nodes encrypt the messages using session keys and hash functions while forwarding the messages and the destination nodes decrypt the messages. This scheme was proved to enhance the PDR by reducing the end to end delay and packet drops.

From the literature review it is evident that machine learning plays a prominent role in optimising the routing process and in detecting the attacks in MANETs. As no much work was done in providing security services for LAR protocol, we have found it meaningful to design a MLAD system to secure LAR in MANETs.

3 LAR and LA

As proposed by Kong and Hong (2003), Lakshmivarahan (1981), Najim and Poznyak (1994) and Narendra and Thathachar (1989), LA is an autonomous learning model that gains knowledge while executing codes and uses that knowledge to identify the future course of actions. In our system, LA is used with LAR to optimise the path selection and to reduce overhead in the network.

3.1 LAR protocol

LAR protocol is a commendable work in the field of MANETs. This routing protocol makes use of location information to identify the requested and expected zone in the network. The request zone includes both the sender and receiver in a rectangular area. Thus a reduction in the search area brings in a greater reduction in the routing over heads.

3.2 Learning automata

As illustrated by Narendra and Thathachar (1989), the learning automaton is represented as quintuple {P, Q, X, Y and Z}, where:

- $P = \{p_1, p_2, p_3, \ldots, p_n\}$ is a set of internal states of the automaton.
- $Q = \{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ is a set of automaton functions.
- $X = \{\beta_1, \beta_2, \beta_3, \ldots, \beta_n\}$ is a set of results obtained from the automaton actions.
- Y is a mapping function between n^{th} and $(n + 1)^{th}$ state inputs of the automaton.
- Z is a mapping function between n^{th} state's response and $(n + 1)^{th}$ state's action.

3.3 Automaton environment

The authors Royer and Toh (1999) have used a triplet {Q, X, C}, where Q and X are as defined earlier and $C\{c_1, c_2, c_3, \ldots, c_n\}$ represents penalty probabilities. Each $c_i \in C$ is proportional to input action α_i. The LA can be defined using an action probability vector Av(t) at time 't', and the average penalty Bp(t) as follows:

$$\begin{aligned}
&P = A \text{ and } M = B \\
&Bp(t) = E\left[\beta(t) \middle| Av(t)\right] = Ar\left[\beta(t) = 1 \middle| Av(t)\right] \\
&= \sum\nolimits_{i=1}^{r} Ar\left[\beta(t) = 1 \middle| \alpha(t) = \alpha_i\right] \times A_r\left[\alpha(t) - \alpha_i\right] \\
&= \sum\nolimits_{i=1}^{r} c_i p_i(t)
\end{aligned} \tag{1}$$

In respect of the ‘pure-chance’ automaton, the average penalty is as shown below.

$$B_0 = \frac{1}{r}\sum_{i=1}^{r} c_i \tag{2}$$

Following are the LA parameters with their description:

- A = $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ is a set feasible paths between two nodes, where α_i is the path at the i^{th} instant
- B indicates the success or failure of the packet delivery. So its value is either 0 or 1
- GV represents a node’s goodness value. If goodness value is high then the PDR also tends to be high
- AG denotes average goodness value by considering all the nodes in a path
- RC is the constant used with reward scheme, where $0 < RC < 1$
- PC is the constant used with penalty scheme, where $0 < PC < 1$
- T denotes the time instant
- HE represents the efficiency of the system
- TH is the threshold value for a path’s goodness.

4 MLAD algorithm

Our MLAD algorithm makes use of the goodness value table, goodness update messages and the reward and penalisation schemes discussed below.

4.1 Goodness value table

In LA, each node maintains a goodness table that records the goodness values of all available paths between source and destination nodes. The entry node actually contains the details of the destination node and the next hop neighbour that lies on the path with maximum goodness value. An update sequence number is used to make any updates on the table. A new update is considered only if its sequence number is found higher than the existing update sequence number. Finally, the path with highest goodness value is calculated based on the reward and penalty schemes discussed below.

4.2 Update message on goodness value

An update message on the goodness value of a node shall be small so as to keep the traffic over head in minimum level. The message should be sent in regular intervals so that the nodes are all in synch with the updated message. Our proposed goodness method will use a header which will perform the task of informing the neighbouring nodes about a particular node's goodness value. We have also modified the table so as to keep the update sequence number as the first element in the table.

Arranging the table in this way paves way for a smoother network and helps in immediate rejection of the messages with old update sequence number. In this way the processing is swift and the other fields in the table need not be checked for evaluation of the incoming message. The goodness update message will be added to the table during the process of route reply message or during packet acknowledgement. So the messages are not repeated and are updated with unique messages.

4.3 Reward scheme

LA will reward the successfully delivered packet at each node using the rewarding scheme as described below.

```
if (node under consideration = destination)
$GV = GV + RC$;
$AG = GV$;
else if ($AG \leq T$ )
$GV = GV + RC$;
$AG = \eta \times GV + (1 - \eta) \times AGn - 1$
else
$GV = GV + RC$;
```

Here, the constant η helps in analysing the weightage of the selected path in terms of its goodness value.

4.4 Penalty scheme

The penalty scheme is applied when there is any packet loss during delivery. The penalty function is as follows.

```
if ( node under consideration = destination)
$GV = GV \times PC$;
$AG = GV$;
else
$GV = GV + RC$;
$AG = \eta \times GV + (1 - \eta) \times AGn - 1$
```

This process is quite similar to the reward scheme and η is also similar to the one used with reward scheme. In MANETs, the mobile nodes make up the entire network and LA at each node will reward or penalise the node depending on the packet delivery report. The value of penalty (P) decides a lot of factors on the network. The value of P is said to range between 0.3–0.5. The tolerance against packet failures depends on the value of P. Higher the value of P, lower is the network's tolerance to faults.

4.5 MLAD algorithm

Initialisation:

RC: 0 < RC < 1

PC: 0 < PC < 1

TH- Threshold on a path's goodness value

Input - Set of available paths

Output - Optimal path in the set of available paths.

Algorithm

1 Let NT be the number of packets transmitted.

2 For each packet to be sent, a path with maximum goodness value is used to forward the packet to its next hopneighbour. Similarly, each intermediate node forwards the packet to the next hop neighbour using the path with maximum goodness value.

3 Upon receiving a packet, the destination node will send an ACK to the sender. All the nodes that receive ACK will get rewarded and others get penalised.

5 Extended ID-based cryptography

5.1 Assumptions

We assume that Alice and Bob are the two communicating nodes and Trent is a trusted third party acting as certificate authority (CA) or PKG for Alice and Bob. Our work is based on the EIBC mechanism proposed by the authors Nicanfar and Victor (2012), where a PRNG and a chain of PMFs are used in addition to the basic elements of ID-based cryptosystems.

- PRNG: linear congruently method is used to implement PRNG with m and n as the PRNG parameters.

$$\begin{cases} \tilde{z}_{i+1} \equiv (m * \tilde{z}_i + n) mod\ r \\ z.t.: i, m, n, q \in \mathbb{Z}, \tilde{z}_i \in \mathbb{Z}_r^* \end{cases} \tag{3}$$

- PMF is defined as below:

  Characteristics over $\mathbb{Z}_r^*$ and G_2

$$\begin{cases} (1) h_i : \mathbb{Z}_r^* \to \mathbb{Z}_r^*, G_1 \to G_1, \forall i \in \mathbb{Z}/0 \\ (2) h_i(z.Q) = h_i(z).h_i(Q), \forall z \in \mathbb{Z}_r^*, \forall Q \in \mathrm{G}_1 & \text{(3a)} \\ (3) H_1^{i+1}(.) = h_{i+1}\left(H_1^i(.)\right) & \text{(3b)} \end{cases}$$

  Equation 3(b) describes the update on system hash function H_1^i. Designing PMF as one-way function derives better results.

5.2 Definitions

EIBC system uses two secret values namely z_i and $\tilde{z}_i$, which are similar to that of the original model. As mentioned earlier, Trent retains z_i and shares PRNG value $\tilde{z}_i$ along with PRNG parameters m and n with Alice and Bob.

The system uses three timers such as short-term refreshment (STR), medium-term refreshment (MTR) and long-term refreshment (LTR) timers.

In our proposed method we use 'live' to indicate system's *i*th state and identifies the current system values and z_i & $\tilde{z}_i$ and H_i & H_1^i.

5.3 EIBC mechanism

Trent will select the secret values $z_i, \tilde{z}_i \in \mathbb{Z}_r^*$, and computes its public key as below:

$$\begin{cases} \breve{P}_0 = h_0(P) & \text{(4a)} \\ P_0 = h_0(\tilde{s}_0).s_0.h_0(P) = h_0(\tilde{s}_0).s_0.\breve{P}_0 & \text{(4b)} \\ \breve{P}_i = h_i(\breve{P}_{i-1}) = h_i(h_{i-1})\Big(\big(h_1(h_0(P))\big)\Big), i > 0 & \text{(4c)} \\ \tilde{P}_i = s_i.\breve{P}_i & \text{(4d)} \\ P_i = h_i(\tilde{s}_i).\tilde{P}_i & \text{(4e)} \end{cases}$$

Li is introduced as a live Trent's public key seed value. It is assumed that Alice and Bob are capable of getting a live public key seed value of Trent. Similarly, Trent gets the hash functions namely H_1^i; H_2 and H_3 and the live values z_i and $\tilde{z}_i$, and parameters m and n as mentioned in equation (10).

So Trent forms the system parameters as shown below by (5).

$$\widehat{\text{Parm}_i}: \begin{cases} H_1^i : \{0,1\}^* \rightarrow G_1 s.t. H_1^{i+1}(.) = h_{i+1}\left(H_1^i(.)\right) \\ H_2 : G_2 \rightarrow \{0,1\}^i, 1 = \max(\text{plain text}) \\ H_3 : G_2 \rightarrow \mathbb{Z}_r^* \\ \widehat{\text{Parm}_i} = \left\{\hat{e}, \breve{P}_i, h_i, H_1^i, H_2, H_3, G_1, G_2, \tilde{s}_i, a, b\right\} \end{cases} \quad (5)$$

The set of equations from equations (6a) to (6d) are used to update the system parameters that align with equation (10).

$$\begin{cases} z_{i+1} = h_{i+1}(z_i) & \text{(6a)} \\ \tilde{L}_{i+1} = z_{i+1}.\breve{L}_{i+1} = h_{i+1}(z_i).h_{i+1}(\breve{L}_i) & \text{(6b)} \\ \tilde{L}_{i+1} = h_{i+1}(z_i.\breve{L}_i) = h_{i+1}(\tilde{L}_i) & \text{(6c)} \\ L_{i+1} = h_{i+1}(\tilde{z}_{i+1}).\tilde{L}_{i+1} = h_{i+1}(\tilde{z}i+1).h_{i+1}(\tilde{L}_i) & \text{(6d)} \end{cases}$$

Alice and Bob can accesses $\widehat{\text{Parm}_i}$, and calculate the live Trent's public key as they have Pi with them. This is shown in equation (4e).Based on the equation (7), Alice and Bob apply H_1^i to find the live public key of other party.

$$LK_A^i = H_1^i(ID_A) \tag{7}$$

- Private key extraction: Trent calculates all the entities, such as seed value of Bob's private key as shown in equation (8), and in turn sends it to the entity (Bob) through a secure channel.

$$\widetilde{L_r K_B^i} = z_i . H_1^i(ID_B) \tag{8}$$

- Computation of the live private key of Bob:

$$L_r K_B^i = h_i(\tilde{z}_i).\widetilde{L_r K_B^i} \tag{9}$$

$$L_r K_B^i = h_i(\tilde{z}_i).z_i.H_1^i(ID_B) = h_i(\tilde{z}_i).z.\widetilde{LbK_B^i} \tag{10}$$

- Verification of Bob's private key:

$$\begin{cases} \hat{e}\left(L_r K_B^i, \breve{L}_i\right) = \hat{e}\left(h_i(\tilde{z}_i).z_i.H_1^i(ID_B), \breve{L}_i\right) \\ = \hat{e}\left(H_1^i(ID_B), \breve{L}_i\right)^{h_i(\tilde{z}_i).z_i} \\ = \hat{e}\left(H_1^i(ID_B), h_i(\tilde{z}_i).z_i.\breve{L}_i\right) \\ = \hat{e}\left(H_1^i(ID_B), h_i(\tilde{z}_i).\breve{L}_i\right) \\ = \hat{e}\left(H_1^i(ID_B), L_i\right) \end{cases} \tag{11}$$

5.3.1 Extended ID-based encryption

Assume that Alice needs to send a message, MS $\in \{0, 1\}^1$ to Bob. To do so, Alice calculates the live public key of Bob. Then a random variable is chosen from $r \in \mathbb{Z}_r^*$, and calculates K and O as below:

$$K = r.\breve{L}_i \tag{12}$$

$$O = MS \oplus H_2\left(\hat{e}\left(L_r K_B^i, L_i\right)^r\right) \tag{13}$$

Finally, C = (K, O) is sent to Bob in the form of encrypted message MS.

5.3.2 Extended ID-base signature

By using H_3 Alice computes σ_i to have her signature for message MS.

$$\sigma_i = H_3(MS).L_r K_A^i \tag{14}$$

Along with the message MS, she sends σ_i to Bob.

The signature is verified by Bob using equation (15).

$$\begin{aligned}
&\hat{e}\left(\breve{P}_i, \sigma_i\right) = \hat{e}\left(\breve{P}_i, \left(H_3(M).\Pr K_A^i\right)\right) \\
&= \hat{e}\left(\breve{P}_i, h_i\left(\breve{r}_i\right).r_i.PbK_A^i\right)^{H_3(M)} \\
&= \hat{e}\left(\breve{P}_i, PbK_A^i\right)^{h_i(\tilde{r}_i).r_i.H_3(M)} \\
&= \hat{e}\left(H_3(M).h_i\left(\tilde{r}_i\right).r_i.\breve{P}_i, PbK_A^i\right) \\
&= \hat{e}\left(H_3(M).P_i, PbK_A^i\right)
\end{aligned} \tag{15}$$

5.4 *Key refreshment*

- STR process: The shared secret value of Trent is refreshed and the hash function is updated. An update on the entire key that includes public and private keys is done as follows.
- Trent: An updated H^i is calculated and shared with Alice and Bob with the new iterative value i, so it becomes i + 1 with valid time (VT_s) which indicates function's start time.
- Alice: Refreshes $\tilde{z}_i$ based on equation (3). H_1^i is refreshed using equation (3b) so that she can obtain new public keys of both Bob and Trent. The updated values of $\tilde{z}_{i+1}$ and H_1^i are considered to refresh the private key of Alice using equation (10).

6 Privacy preserving communications

Dynamic flow identification, random node identification and resilient packet forwarding are the three ways in which privacy can be preserved over communication.

Dynamic flow identification eliminates the chances of identifying source and destination nodes. Random node identification is employed to isolate the identity of a node from its location. Resilient packet forwarding is introduced to target at hectic networks to analyse the attacks in the traffic.

The following terminology is considered throughout the process:

SR	stands for sender and receiver which are equivalent to source and destination
DE	destination identifier
N	average count of neighbouring hubs in the communication range
P_{Si}	*i*th flow pseudonym of source
P_{Di}	*i*th flow pseudonym of destination
K_{ij}	symmetric key between hubs i and j
E_{Ky} SR(.)	encryption using Ky as a key
D(K_{SD}) (.)	decryption using K_{SD} as a key

In our system, the assaults such as packet tracing, packet counting, timing and time-to-live (TTL) are considered to accompany the activity examination process.

6.1 Dynamic flow identification

Traditional MANET protocols embed source and destination nodes' address in the data packets. Any adversaries present in the route may lead to prediction of the location of the nodes. We have proposed a network flow which does not reveal the source and destination addresses. This is achieved using dynamic flow identification developed on the top of forward chaining. This mechanism uses and as bidirectional flow pseudonyms. These pseudonyms replace identity of source and destination nodes in packets. These pseudonyms are broadcasted through the source as RREQ packet.

$$< \mathrm{RREQ}, P_{Si}, P_{Di}, E_{K_Y}SR(.) > .$$

Upon receiving the RREQ packets, each intermediate node decrypts and interprets the flow pseudonyms. This unmasks the source and destination nodes identity by opening the trapdoor. A node that receives the RREQ uses the P_{Di} to check whether it is the intended destination or not. If the node is not the intended destination, then it makes an entry to the routing table for initiating backward flow using P_{Si}. As each intermediate node has to undergo trapdoor check, it is required to keep this process more efficient. The symmetric key along with the identifiers of source and destination nodes helps in determining the initial pseudonyms P_{D0} and P_{S0}. Always there is a liberty for the source and destination to modify the flow pseudonyms at any point of time. The forward chaining process mentioned below aids in determining successive flow pseudonyms.

$$P_{S0} = f_{K_Y}(SR) \rightarrow P_{S1} = f_{K_Y}(P_{S0}) \ldots \rightarrow P_{Sn} = f_{K_Y}(P_{Sn-1})$$
$$P_{D0} = f_{K_Y}(DE) \rightarrow P_{D1} = f_{K_Y}(P_{D0}) \ldots \rightarrow P_{Dn} = f_{K_Y}(P_{Dn-1})$$

Here f is a one-way hash function powered with cryptographic key as specified by the authors Sumalatha and Sathyanarayana (2015). The result of this function f is kept simple and random for each intermediate node. The complete process of trapdoor check is kept simple and light weighted. RREQ message processing needs trapdoor check to fix up flow. Once the flow is established, no additional trap checks are needed for forwarding consequent packets. Binary search tree is adopted to optimise the data structure used by the trapdoor process.

6.2 Random node identification

The objective in using random node identification is to hide the identity of a node from its location thereby making the route tracing difficult. Each mobile node uses randomly generated layer 2 and layer 3 addresses as random node identifier (RNI). The RNI is advertised through messages similar to the HELLO message in AODV (Perkins and Royer, 2003). Neighbouring node identification happens only through their RNIs to ensure that routing and communication happens through the neighbouring nodes. The RNI is changed at random time intervals to prevent the attackers and adversaries from learning the physical location of the source and destination nodes.

In case of pseudonyms, source and destination nodes need not know the RNI of each other. The benefit in doing so is twofold. Firstly, the RNI of source and destination may change independently and secondly, the location of source and destination cannot be revealed as they do not know each other's RNI.

Since the RNI changes at random intervals and is independent by itself, it is difficult for adversaries to trace the changes or predict the RNI of a node. One major fault in this method is that there are chances where two nodes can chose the same RNI. But the probability of generating same RNI (48 bit MAC address and 32 bit layer 3 addresses) by any two nodes is very less.

$$\left(\frac{1}{2^{48}}\frac{1}{2^{32}}=\frac{1}{2^{80}}\right)$$

6.3 Resilient packet forwarding

We have proposed a traffic forwarding scheme that safeguards the communication from eavesdropping. This method comprises of multi-path random forwarding (MPRF), random time-to-live (RTTL) and hint.

- MPRF

  Networks with sparse traffic and less mobility are more prone to attacks as the paths are used for a prolonged time. To forward a packet, each intermediate node decides the route on random basis and selects a next hop. Lee and Gerla (2001), Marina and Das (2001) and Ye et al. (2003) have specified that multi-path routing delivers good quality of service and reliability. However, in multipath routing, there will be link/node disjoint paths that lead to eavesdropping. The attacker easily gains the packet count and reconstructs the end-to-end paths. In order to mitigate this vulnerability and to institute stable multi-paths we allow non-disjoint paths.

- RTTL

  TTL eliminates the packets that could not find their destination. A source node initialises TTL with the length of the path and its value is decreased by 1 by each node in the path. Thus the relative position of a node in the path, either from source or destination can be predicted. RTTL is proposed to avoid the ill behaviour of compromised nodes. In this case, TTL is set to a random value and RTTL is the sum of the randomly chosen TTL value and the length of the path.

  The initial random value of TTL is enclosed in the encrypted data packet by the source node. As a regular process the TTL value will be decreased by 1 by each node in path during transit. The position of the node cannot be interpreted as the TTL value is initialised with a random value. The destination node receives this encrypted packet with the RTTL value. It validates the received RTTL by simply subtracting the initial random value from the RTTL.

6.4 Security analysis

This section reveals internal attacks and the corresponding counter mechanisms offered by PPCS.

- *Internal attackers:* Intermediate node acting as an adversary node accesses various fields of a packet and collates information such as pseudonym, TTL, next and previous hop neighbours. With this information the intermediate node restructures the entire network path. Thus it is easy for the intermediate node to guess the source and destination nodes (Kong and Hong, 2003).

A mathematical equation is derived to demonstrate the probability of the set of intermediate nodes that can successfully draft the network path. Following are the notations used in deriving the equation.

- ND: number of nodes
- CM: compromised nodes
- APL: average path length
- TN: uncompromised nodes in the route
- WN: intermediate nodes between the source and destination
- G: (ND − CM) − TN
- p: probability of a node to get compromised
- $P_{\text{first, src}} = P_{\text{last, dest}}$: probability of first or last hop node guessing the Src or Dest node
- $P_{\text{int, src}} = P_{\text{int, dest}}$: probability of an intermediate node guessing the Src or Dest node
- $P_{\text{int + first, link}} = P_{\text{int + last, link}}$: probability of first or last hop node along with an intermediate node guessing the link between Src and Dest nodes
- $P_{\text{first + last, link}}$: probability of first or last hop node predicting the link between Src and Dest node
- $P_{\text{int + int, link}}$: probability with which the intermediate nodes collectively guesses the link between the Src and Dest nodes.

Pb(a = src) and Pb(a = dest) denotes the probability with which an attacker identifies the source and destination respectively. Pb(a = (src, dest)) denotes the probability with which an attacker finds both source and destination.

The probability of finding the source and destination node by a compromised node depends on its position in the path. The probability is high when the compromised node is either the first hop or last hop node.

In our work, we use four cases of node compromise for a path that has ‘n’ compromised nodes.

Case 1 First hop and zero or more other nodes are compromised

Probability of Case 1: $P1 = P(a \mid C1)\, P(C1)$

where $P(C1) = (1 - p)^{APL - n}\, p^{n}(APL - 2, n - 1)$.

Case 2 Last hop and zero or more other nodes are compromised

Probability of Case 2: $P2 = P(a \mid C2)\, P(C2)$

where $P(C2) = (1 - p)^{APL - n}\, p^{n}(APL - 2, n - 1)$.

Case 3 First hop node, last hop node and zero or more other nodes are compromised

Probability of Case 3: $P3= P(a \mid C3)\, P(C3)$

where $P(C3) = (1 - p)^{APL - n} p^n(APL - 2, n - 2)$.

Case 4 One or more nodes other than first, last hop nodes are compromised

Probability of Case 4: $P4 = P(a \mid C4) P(C4)$

where $P(C4) = (1 - p)^{APL - n} p^n(APL - 2, n)$.

Thus the probability of an attacker finding target anonymity, $P(a) = P1 + P2 + P3 + P4$.

In disjoint multi path environments, the probability is defined as: $P_m(a) = 1 - (1 - P(a))^R$, where R is the total number of disjoint paths.

7 Methodology

We have used LA with LAR to optimise the path selection and to reduce overhead in the network. LAR makes use of location information to identify the requested and expected zone in the network. The request zone includes both the sender and receiver in a rectangular area. This reduction in the search area brings in a greater reduction in the routing overhead. We have proposed a MLAD algorithm that uses multipath routing to facilitate efficient routing even in the presence of attackers. This scheme makes use of the goodness value table, goodness update messages and the reward and penalisation schemes to efficiently detect and isolate attackers. The goodness update messages are added to the table during the process of route reply message or during packet acknowledgement. So the messages are not repeated and are updated with unique messages. The path with highest goodness value is calculated based on the reward and penalty schemes. LA will reward the paths based on the rewarding scheme and the penalty scheme is applied to penalise a path when there is any packet loss during delivery. EIBC is used for efficient key management in providing system security. The EIBC mechanism proposed by the authors Nicanfar and Victor (2012) uses a PRNG and a chain of PMFs in addition to the basic elements of ID-based cryptosystems. The EIBC mechanism comprises of extended ID-based encryption (EIBE) and extended ID-base signature (EIBS) schemes. The proposed system also implements PPCS for maintaining privacy in end-to-end communication. This method decouples the location information from the node's identifier and abstracts the communication happening among nodes. Schemes such as dynamic flow identification, random node identification and resilient packet forwarding are used for privacy preservation over communication. Dynamic flow identification eliminates the chances of identifying source and destination nodes, random node identification isolates the identity of a node from its location and resilient packet forwarding targets at hectic networks to analyse the attacks in the traffic. In our system, the assaults such as packet tracing, packet counting, timing and TTL are considered to accompany the activity examination process. We have proposed a network flow which does not reveal the source and destination addresses. This is achieved using dynamic flow identification developed on the top of forward chaining that uses random node identification. The objective in using random node identification is to hide the identity of a node from its location thereby making the route tracing difficult. The system also adopts resilient packet forwarding that safeguards the communication from eavesdropping. This method comprises of MPRF, RTTL and hint. In order to detect internal attackers, certain intermediate nodes acts as adversary nodes to access various fields of a packet and collate information such as pseudonym, TTL, next and previous hop neighbours. This information helps the intermediate nodes to restructure the entire network path. Thus it is easy for the intermediate node to guess the source and destination nodes. A mathematical equation is derived to demonstrate the probability of the set of intermediate nodes that can successfully draft the network path. Thus, our proposed MLAD system integrates LA, EIBC and PPCS methods with LAR to facilitate efficient and secure LAR in MANETs.

8 Performance evaluation

We have performed simulations in NS-2 using C++ as the tool command language. Varied node densities were considered over an area of 1,000 square metres. MAC layer and radio models of IEEE 802.11 standard were used for simulation. At data communication level, the processing of network data is very expensive. Hence, the experiments were conducted without considering the overhead caused by multicast members leaving the group. The simulation parameters used in our system are listed in Table1.

Table 1 Simulation parameters

Parameter	*Value(s)*
Area	1,000 m * 1,000 m
No. of nodes	50, 100, 150, 200
Type of mobility	Random way point
Speed of mobility	5, 10, 15, 20, 25 m/s
Pause time	5 ms
Type of propagation	Two ray ground
MAC type	802.11
Routing protocol	LAR-EIBC, LAR, LAR-ML, LAR-PP_EIBC_ML
No. of attackers	5, 10, 15, 20, 25
Type of traffic	CBR
Traffic sources	5, 10, 15, 20, 25

Simulations were carried out with four types of routing schemes in the presence of attackers.

1 LAR without security (LAR-MALICIOUS)

2 LAR using extended ID-based cryptography (LAR-EIBC)

3 LAR using machine learning (LAR-ML)

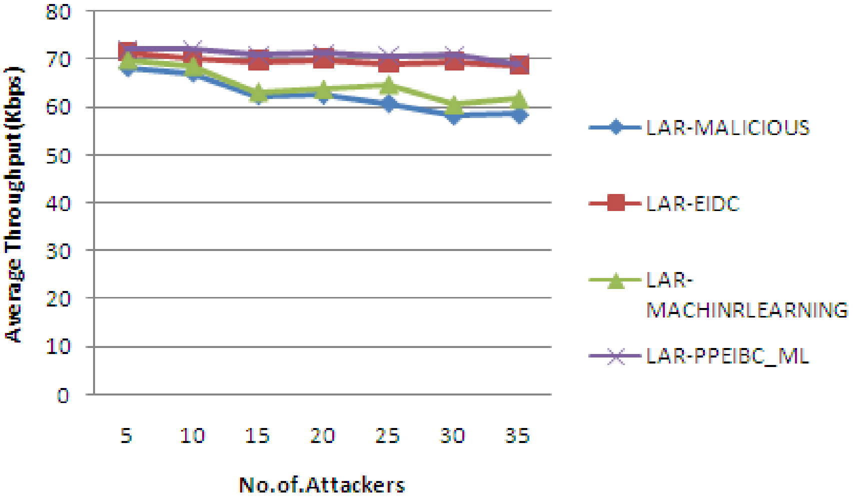
4 LAR using privacy preservation, EIBC and machine learning (LAR-PP_EIBC_ML)

The performance of the proposed system with privacy preservation, EIBC and machine learning was compared with other schemes based on the performance metrics throughput, PDR, routing overhead, end to end delay and packet loss.

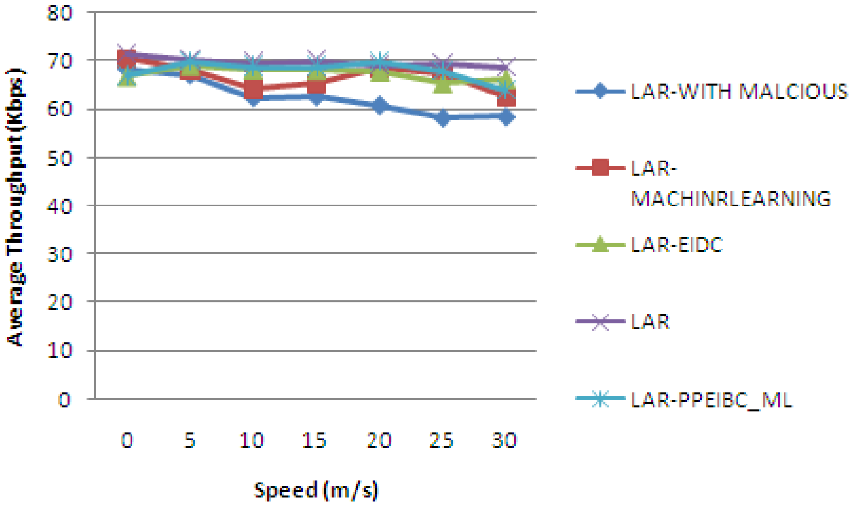
8.1 Throughput

From the graphs shown in Figure 1(a) and Figure 1(b) it is evident that our system delivers the highest average throughput compared to other systems. An average throughput of 62 Kbps was obtained with varied number of attackers. Also our system recorded an average throughput of 61 Kbps with varied node speeds.

Figure 1 (a) Throughput vs. no. of attackers (b) Throughput vs. speed (see online version for colours)



(a)

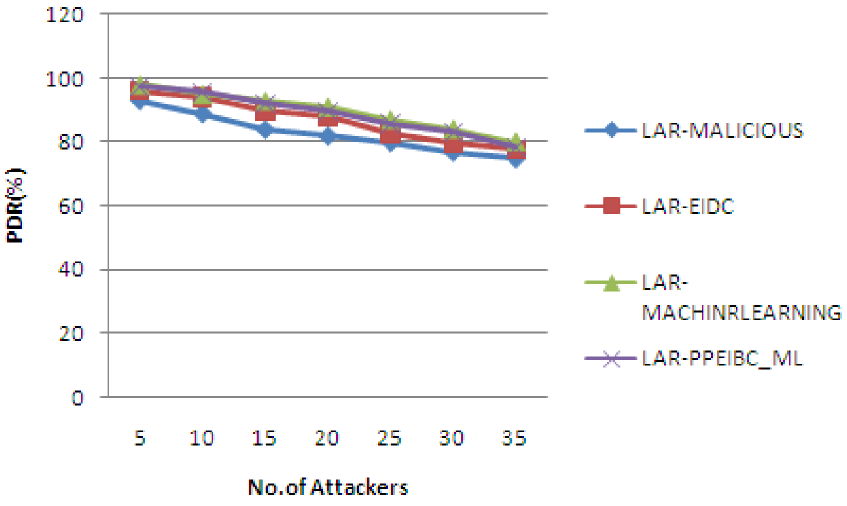


(b)

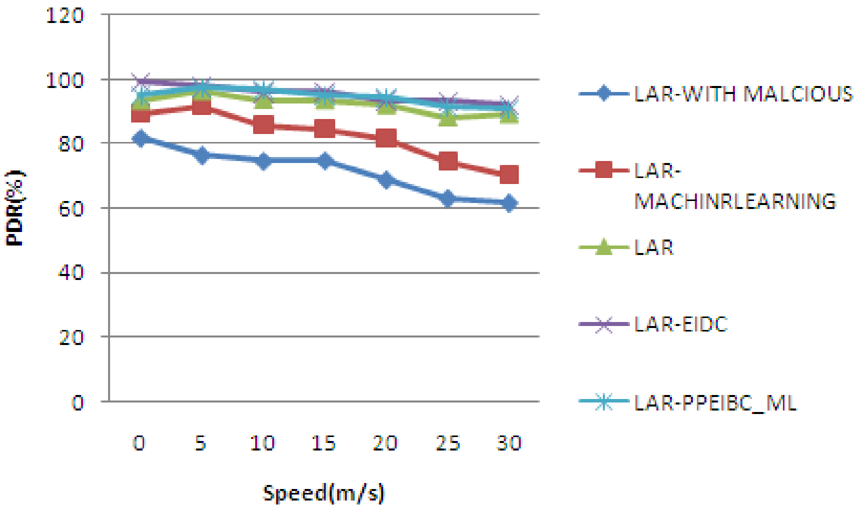
8.2 Packet delivery ratio

From the graphs shown in Figure 2(a) and Figure 2(b) it is evident that an average PDR of 81% is recorded with varied number of attackers and an average PDR of 72% is registered with varied node speeds.

Figure 2 (a) PDR vs. no. of attackers (b) PDR vs. speed (see online version for colours)



(a)

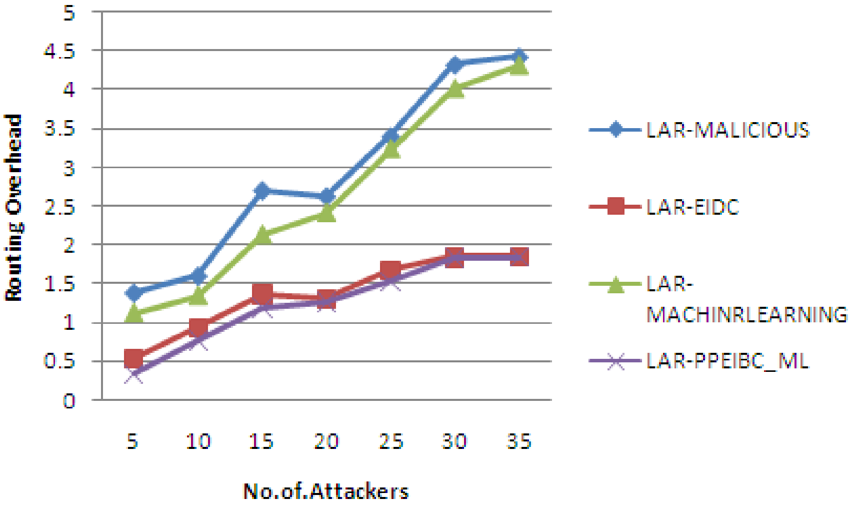


(b)

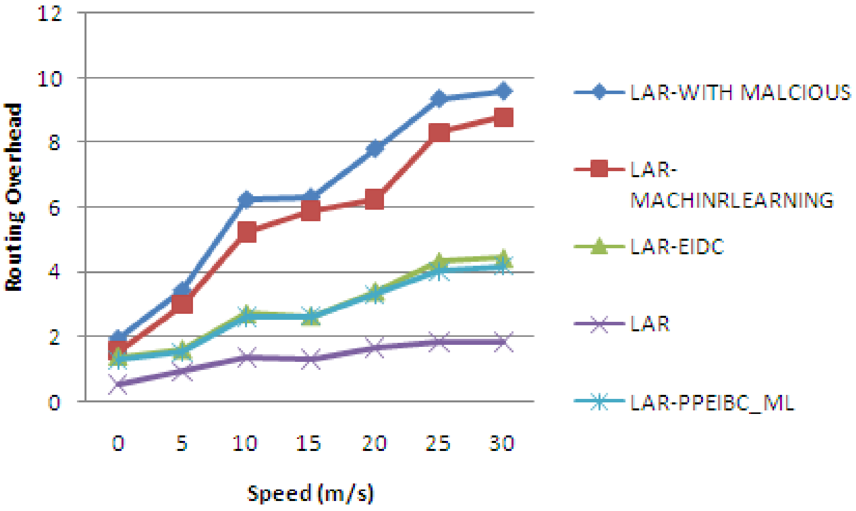
8.3 Routing overhead

From the graphs shown in Figure 3(a) and Figure 3(b) it is evident that our system has resulted in a significant drop in routing overhead.

Figure 3 (a) Routing overhead vs. no. of attackers (b) Routing overhead vs. speed (see online version for colours)



(a)

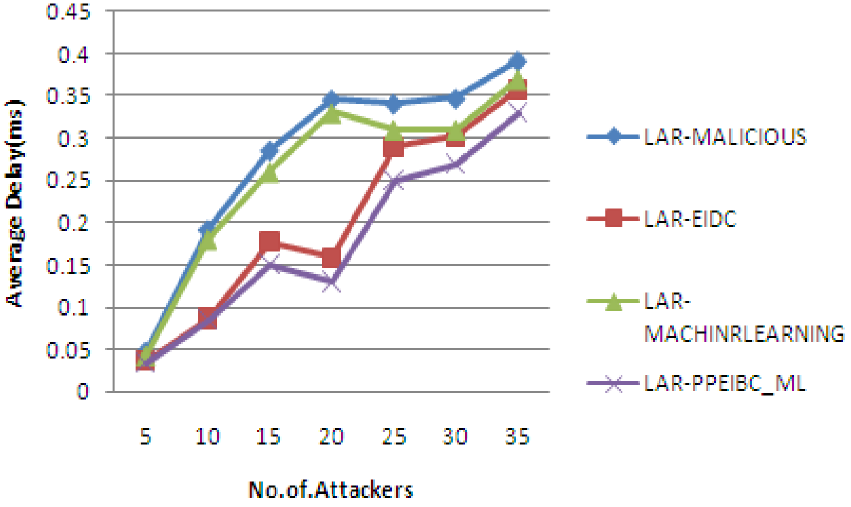


(b)

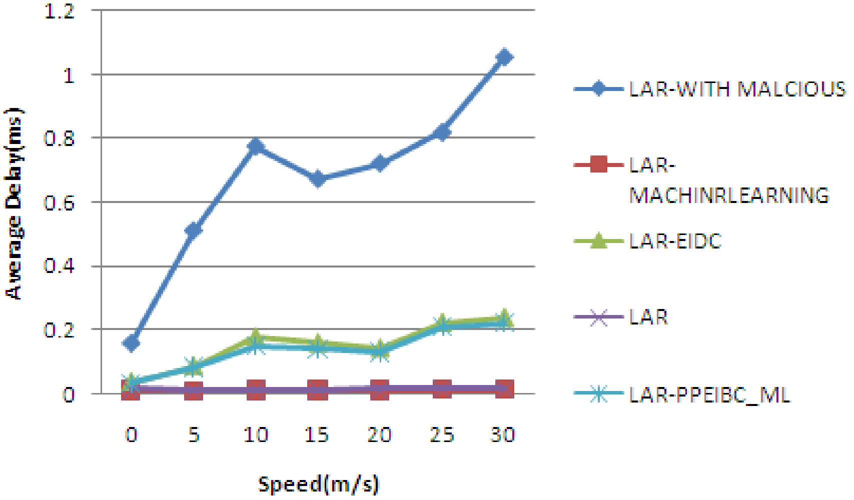
8.4 Average end-to-end delay

From the graphs shown in Figure 4(a) and Figure 4(b) it is noticed that our system has decreased the average end-to-end delay with varied number of attackers and at varied node speeds.

Figure 4 (a) Average delay vs. no. of attackers (b) Average delay vs. speed (see online version for colours)



(a)

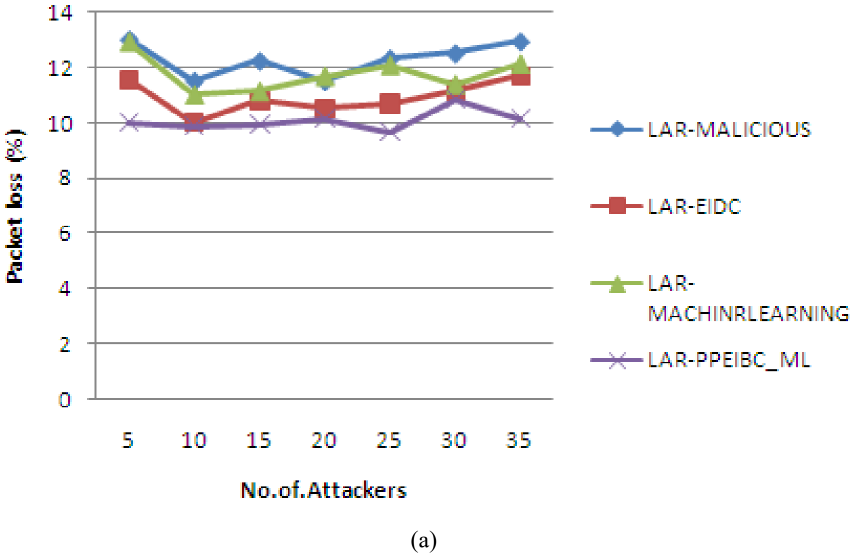


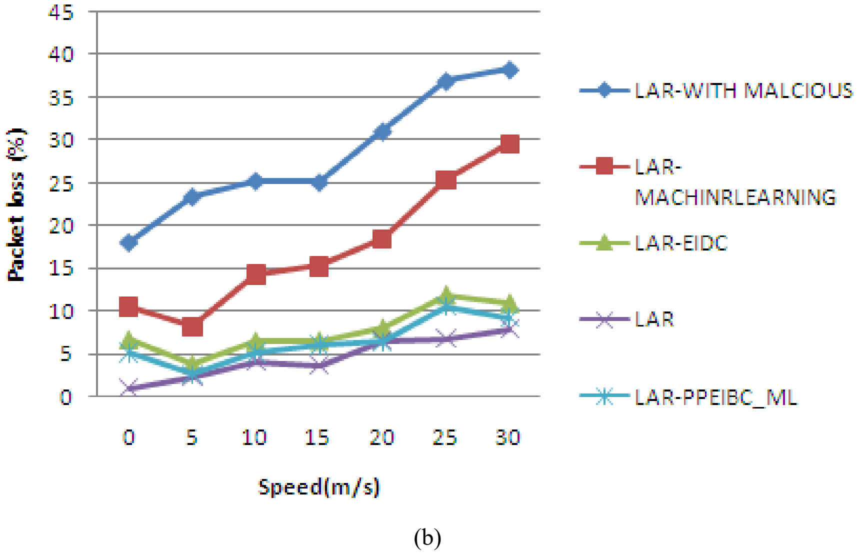
(b)

8.5 Packet loss

From Figure 5(a) and Figure 5(b) it is observed that our system has considerably reduced the Packet Loss with varied number of attackers and at varied node speeds.

Figure 5 (a) Packet loss vs. no. of attackers (b) Packet loss vs. speed (see online version for colours)





9 Discussions and conclusions

In recent years MANETs are gaining popularity due to the availability of low cost advanced wireless communication hardware and underlying technologies. MANETs play a vital role in real time applications such as military tactical operations, search and rescue operations, disaster relief operations and law enforcement. As MANETs are infrastructure less networks without any centralised administration, it is obvious that the participating nodes act as routers to form an autonomous ad hoc network. The factors such as open medium, widespread nodes, frequently changing topologies and lack of centralised administration makes MANETs an ideal target for attackers. Hence, security services are required to safeguard the network from the malicious activities of the attackers. There is an ample scope for the attackers to introduce malicious or non-cooperative nodes into the network. To safeguard the MANET communications from those security attacks, we have proposed a MLAD system. The current work had resulted in good improvisation of the performance of location-based routing in MANETs. The proposed MLAD algorithm uses multi path routing and is found efficient in the presence of attackers. The adoption of LAR in our system has optimised the search process, reduced the search area for new routes and thereby enhanced the life of mobile hosts. The proposed LA augmented the performance of LAR in optimising the path selection and in reducing network overhead. The extended identity-based cryptography (EIBC) acted as an efficient key management scheme while providing system security and it had resulted in the reduction of eavesdropping. In order to safeguard node privacy, a PPCS is used to encrypt and decrypt data so as to prevent hackers and their attacks. Our system had used an optimal guessing strategy on attacks and proved that the guessing strategy works independent of the path's node density. The perseverance of PPCS against passive internal attacks and also its strength against external attacks is proved. The results of the simulated process had practically showcased the efficiency of the system with minimal impact on packet delivery. Route selection and route evaluation methods were introduced for fault tolerance routing. These methods helped in finding the probability of successful route selection and packet delivery. Our scheme had combined fault tolerant routing and cluster routing methods to achieve optimal state in terms of minimised overheads, malicious activities and broken path issues. Simulations were carried out in NS2 and the performance of the proposed system that integrates privacy preservation, EIBC and machine learning was compared with other schemes. The result analysis had revealed the strength and reliability of our system in securing LAR in MANETs. Our further work aims at introducing multi-level id-based cryptography to secure the authentication of digital signatures.

References

Athreya, A.P. and Tague, P. (2011) 'Towards secure multi-path routing for wireless mobile ad-hoc networks: a cross-layer strategy', in *Proceedings of 8th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks (SECON)*, pp.146–148.

Corson, S. and Macker, J. (1998) 'Mobile ad hoc networking (MANET): routing protocol performance issues and evaluation considerations', *Internet-Draft*, March.

Corson, S., Batsell, S. and Macker, J. (1996) 'Architectural considerations for mobile mesh networking', *Internet-Draft RFC*, Version 2, May.

Huang, Y. and Lee, W. (2003) 'A cooperative intrusion detection system for ad hoc networks', in *Proceedings of the 1st ACM Workshop on Security of Ad hoc and Sensor Networks, SASN '03, ACM*, New York, NY, USA, pp.135–147.

Huang, Y-A. and Lee, W. (2004) 'Attack analysis and detection for ad hoc routing protocols', in *Proceedings of the Recent Advances in Intrusion Detection, Lecture Notes in Computer Science*, Vol. 3224, Springer, pp.125–145.

Jiang, M., Li, J. and Tay, Y-C. (1998) 'Cluster based routing protocol (CBRP) functional specification', *Internet-Draft*, August.

Johnson, D., Maltz, D.A. and Broch, J. (1998) 'The dynamic source routing protocol for mobile ad hoc networks', *Internet-Draft*, March.

Joseph, J.F.C., Das, A., Seet, B–C. and Lee, B–S. (2007) 'Cross layer versus single layer approaches for intrusion detection in MANETs', *IEEE*, pp.194–199.

Joydipa, S. and Vinodha, K.A. (2013) 'Weighted learning automata-based multicast routing protocol for wireless MANET', *International Journal of Engineering Research & Technology (IJERT)*, June, Vol. 2, No. 6, pp.2230–2235.

Ko, Y-B. and Vaidya, N.H. (1998) *Location-aided Routing in Mobile Ad Hoc Networks*, Technical Report 98-012, CS Dept., Texas A&M University, June.

Ko, Y-B. and Vaidya, N.H. (2000) 'Location-aided routing (LAR) in mobile ad hoc networks', *Wireless Networks*, Vol. 6, No. 4, pp.307–321.

Kong, J. and Hong, X. (2003) 'ANODR: anonymous on demand routing with untraceable routes for mobile ad-hoc networks', in *ACM MOBIHOC*.

Kotov, V. and Vasilev, V. (2011) 'A survey of modern advances in network intrusion detection', in *Proceedings of 13th International Workshop on Computer Science and Information Technology CSIT*, 2011, pp. 18–21, 2011.

Krishna, P., Chatterjee, M.N., Vaidya, H. and Pradhan, D.K. (1995) 'A cluster-based approach for routing in ad hoc networks', Paper presented at *USENIX Symposium on Location Independent and Mobile Computing*, April.

Lakshmivarahan, S. (1981) *Learning Algorithms: Theory and Applications*, Springer, New York.

Lee, S-J. and Gerla, M. (2001) 'Split multipath routing with maximally disjoint paths in ad hoc networks', in *Proceedings of IEEE International Conference on Communications*.

Marina, M.K. and Das, S.R. (2001) 'AOMDV: ad hoc on-demand multipath distance vector routing protocol', in *Proceedings of IEEE ICNP*.

Najim, K. and Poznyak, A.S. (1994) *Learning Automata: Theory and Applications*, Pergamon Press, Oxford.

Narendra, K.S. and Thathachar, M.A.L. (1989) *Learning Automata*, Prentice-Hall, New York.

Nicanfar, H. and Victor, C.M.L. (2012) 'EIBC: enhanced identity-based cryptography, a conceptual design', in *Proceedings of IEEE International Systems Conference (SysCon 2012)*, pp.1–7.

Perkins, C. and Royer, E. (2003) *Ad Hoc On-demand Distance Vector (AODV) Routing*, IETF RFC 3561 [online] http://www.ietf.org/rfc/rfc3561.txt (accessed 24 August 2017).

Rajkumar, B. and Narsimha, G. (2016), 'Secure multipath routing and data transmission in MANET', *International Journal of Networking and Virtual Organisations (IJNVO)*, Vol. 16, No. 3, pp.307–321.

Roopa, M. and Selvakumar, R.S. (2017) 'An intelligent network algorithm for enhanced security in a mobile ad hoc network', *International Journal of Networking and Virtual Organisations (IJNVO)*, Vol. 17, Nos. 2/3, pp.126–136.

Royer, E.M. and Toh, C-K. (1999) 'A review of current routing protocols for ad hoc mobile wireless networks', *IEEE Pers. Commun.*, Vol. 6, No. 2, pp.46–55.

Saju, P.J. and Samuel, P. (2017) 'Trust prediction model for certificate exchange and revocation in MANET', *International Journal of Networking and Virtual Organisations (IJNVO)*, Vol. 17, Nos. 2/3, pp.268–289.

Sen, S. and Clark, J.A. (2008) *Intrusion Detection in Mobile Ad Hoc Networks*, pp.427–454, Springer.

Sen, S. and Clark, J.A. (2009) 'A grammatical evolution approach to intrusion detection on mobile ad hoc networks', in *Proceedings of the Second ACM Conference on Wireless Network Security, WiSec'09, ACM*, NY, USA, pp.95–102.

Sen, S., Clark, J.A. and Tapiador, J.E. (2010) 'Power-aware intrusion detection in mobile ad hoc networks', in *Proceeding of the Ad Hoc Networks, Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering*, Vol. 28, Springer, Berlin/Heidelberg, pp.224–239.

Senthil, K.R. and Kamalakkannan, P. (2013) 'A review and design study of cross layer scheme based algorithm to reduce the link break in MANETs', in *Proceedings of IEEE International Conference on Pattern Recognition, Informatics and Mobile Engineering*, pp.139–143.

Shrestha, R., Han, K-H., Choi, D-U. and Han, S.J. (2010) 'A novel cross layer intrusion detection system in MANET', in *Proceedings of IEEE 14th International Conference on Advanced Information Networking and Applications*, pp.647–654.

Smail, O., Cousin, B. and Snoussaoui, I. (2017) 'Energy-aware and stable cluster-based multipath routing protocol for wireless ad hoc networks', *International Journal of Networking and Virtual Organisations (IJNVO)*, Vol. 17, Nos. 2/3, pp.229–251.

Su, M-Y. (2011) 'Prevention of selective black hole attacks on mobile ad hoc networks through intrusion detection systems', *Computer Communications 2011*, Vol. 34, No. 1, pp.107–117.

Sumalatha, P. and Sathyanarayana, B. (2015) 'Enhanced identity based cryptography for efficient group key management in WSN', *International Journal of Application or Innovation in Engineering & Management*, Vol. 4, No. 6, pp.116–128.

Sun, B., Wu, K. and Pooch, U. (2006) 'Zone-based intrusion detection system for mobile ad hoc networks', *International Journal of Ad Hoc and Sensor Wireless Networks*, Vol. 2, No. 3, pp.2003–2009.

Ye, Z., Krishnamurthy, S.V. and Tripathi, S.K. (2003) 'A framework for reliable routing in mobile ad hoc networks', in *Proceedings of IEEE INFOCOM.*

Zhang, Y. and Lee, W. (2000) 'Intrusion detection in wireless ad-hoc networks', in *Proceedings of the 6th Annual International Conference on Mobile Computing and Networking, MobiCom, ACM*, New York, NY, USA, pp.275–283.

Zhang, Y., Lee, W. and Huang, Y. (2003) 'Intrusion detection techniques for mobile wireless networks', *Wireless Networks 2003*, Vol. 9, No. 5, pp.545–556.