IIOAB JOURNAL
ISSN: 0976-3104

ARTICLE

AN EFFICIENT APPROACH FOR PRIVACY PRESERVING AND DETECTION OF SELECTIVE PACKET DROPPING ATTACKS IN WIRELESS AD HOC NETWORKS

Bhavana Venkatachala Moorthy[1]*and Navamani Thandava Meghanathan

Dept. of Computer Science and Engineering, Easwari Engineering College, Chennai, INDIA

ABSTRACT

Security plays the most important issue that has gained attention by a lot of research and development effort in past few years. In multi-hop wireless ad hoc networks link error and malicious packet dropping are two sources for packet losses which results in denial of service. The main objective of this work is to develop an accurate algorithm for detecting selective packet drops made by insider attackers and to improve the detection accuracy, to differentiate whether packet loss is caused due to link error or activity of the attacker by exploiting the correlations between lost packet and to detect packet dropping attacks in mobile environment. The proposed system observes a sequence of packet losses in the network and interested in determining whether the losses are caused by link errors only or by the combined effect of link errors and malicious drop. It specially considers about the insider attack case, whereby malicious nodes that are part of the route use their knowledge of the communication context to selectively drop small amount of packets critical to the transmission. The existing algorithms that are based on detecting the packet loss rate cannot achieve satisfactory detection accuracy while the packets are dropped selectively and also in frequently changing topology. Hence to improve the detection accuracy, the correlations between the bitmap generated are calculated and lost packets are identified. The public auditing architecture is developed that detects and verifies the truthfulness of the packet loss information reported by nodes. In case of mobile nodes, mobility is also one of the reasons for packet loss. Hence, the proposed detection scheme is attack resilient to different kinds of network environments such as static and mobile network. After running the simulation, we observe that the proposed mechanism achieves better detection accuracy, lower computation complexity and overcomes communication overhead.

KEY WORDS
Wireless ad hoc network, Privacy, Selective Packet Dropping, Auditing, Attack Detection

Received: 13 August 2016
Accepted: 18 August 2016
Published: 12 Sept 2016

***Corresponding Author**
Email:bhavana.cse27@gmail.com
Tel.: +91-9943095133

INTRODUCTION

A wireless ad hoc network is known as a type of decentralized wireless network. The network is ad hoc because it is structure less. As it is structure less it does not have a defined pre existing infrastructure, such as routers in wired networks or access points in managed wireless networks. Inspite, all nodes participate in routing by forwarding data for other nodes, so the determination of which nodes forward data is identified on the basis of network connectivity.

Security is the vital problem in the wireless ad hoc network. Wireless ad hoc network can be affected by various types of attacks [1]. It may contain node which is a part of a route, itself as an attacker. Wireless links in wireless ad hoc network are more prone to active attacks, passive attacks and message distortion. There are different types of attacks such as greyhole attack, blackhole attack, sinkhole attack etc. In this work, we detect the occurrence of greyhole attack which is also known as selective packet dropping attack. In this type of attack, the malicious node drops the packets selectively and also intentionally sometimes. A malicious node which is the part of the route with the knowledge about the network protocol can degrade the performance by launching an insider attack [2]. Specifically, the malicious node may evaluate the importance of various packets, and then drop the small amount of selected packets that are known to be highly critical to the operation of the network. By targeting these highly critical packets, intermittent insider attackers can cause significant damage to the network with low probability of being caught.

[Fig.1] shows the system architecture of Wireless Ad Hoc Network. It shows one source node, one destination node, many intermediate nodes and few auditor nodes. The auditor node is an external node which is not the part of a routing path. As shown in [Fig.1], when the packets are transmitted from the source node to the destination node through the intermediate nodes, there may be packet loss. This packet loss may be due to link error or malicious node. Hence, the auditor node is used to detect the reason for packet loss.

In this work, the destination node calculates the packet loss and if the packet loss rate is beyond the threshold level then the destination node sends request to the intermediate nodes randomly and verifies the reply produced by those nodes. Based on the packets received at those intermediate nodes, the destination node creates a suspect list and sends it to the Auditor node along with the Attack Detection Request (ADR). We develop an accurate algorithm for detecting selective packet drops made by insider attackers in Wireless Ad Hoc Networks which is an improved version of the approach discussed in [2]. Our algorithm also provides a truthful and accurately verifiable decision as a proof to support the detection decision. The high detection accuracy is achieved by calculating the correlations between the positions of lost packets, as calculated from the Auto-Correlation Function (ACF) of the bitmap generated by each node—a bitmap describing the lost/received status of each packet in a sequence of consecutive packet transmissions [2]. Here we propose the extension of our previous work [3] to detect the selective packet dropping attacks with implementation and performance analysis. Here, we face another challenge of detecting the truthfulness of bitmap reported

IIOAB JOURNAL
ISSN: 0976-3104

by each node. This is solved by auditing method which is carried out by the auditor node. The auditor node should not be the part of the route used to carry the packet from source node to destination node.

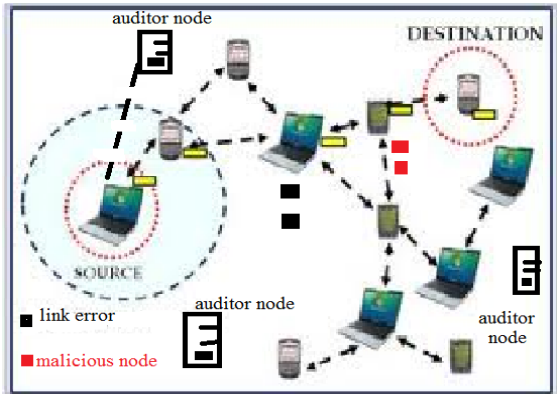

Fig.1: System Architecture of Wireless Ad Hoc Network

The major contributions of this work are as follows: 1) An Extended Homomorphic Linear Authenticator (HLA) approach is proposed for preserving privacy during auditing process and also for securely collecting the information from nodes. 2) An improved auditing method for wireless ad hoc networks is proposed to minimize communication overhead 3) A new algorithm for verification of packet loss is proposed to create suspected node list which can be used for auditing 4) To improve attack detection accuracy, multiple auditor nodes are maintained and implementation is done. 5) An attack detection process is designed to detect selective packet dropping attacks during dynamic mobile environment. The remainder of the paper is described as follows, Section 2 discuss about the related works, in Section 3, we discuss about the proposed system, Section 4 explains about the analysis made on security and communication overhead, in Section 5 we discuss about the performance evaluation and the conclusion in Section 6.

MATERIALS AND METHODS

Preserving privacy and providing security against internal attacks are evolving challenges in wireless ad hoc network. Researchers have worked on these areas and proposed many solutions to address the above issues. However addressing selective packet dropping attack which is a serious threat caused by internal malicious nodes and preserving privacy in wireless ad hoc networks have been given little attention only. In this section, the existing mechanisms for preserving privacy and providing security in wireless networks are discussed.

In [2] & [4], it is considered that packet loss is caused by link error and also by packet dropping. By comparing the number of packets sent and number of packets received, packet loss is detected. Detection algorithm is used to compare the traffic rate with source traffic rate and estimated traffic rate and decide the reason whether packet loss is caused due to link error or malicious packet dropping. All the nodes which are interested to be a part of route should be fully cooperative. But some nodes behave selfishly and get only their benefits and do not share the data with other nodes. Due to continuous mobility of the node, the performance of network gets affected and leads to denial of service. To detect such node which degrades the performance by dropping packets acknowledgement method is used [4]. In [5] & [6], new Intrusion Detection System (IDS) based on Mobile Agents has been designed. This approach uses a set of Mobile Agents (MA) that can move from one node to another node within a network. This method takes much time to detect the malicious nodes. It leads to complexity in calculating the mobile agent.

In [7] & [8] the authors have designed the solution to overcome the problem of selective jamming attacks in wireless networks and examine the cryptographic primitives and neutralizes the inside knowledge of the attackers. In this work, only external attackers are detected and fail to find insider attacks. In [9] & [10], the authors have used trust evaluation method based on the feedbacks collected from neighbour nodes. Hence, these feedbacks are not efficient for detecting selective dropping attacks. In [11] & [12], the authors have classified attack detection system into two categories based on the detection algorithm. The first category considers that packet loss is caused mostly by malicious dropping. The first category is further divided into four sub-categories based on their methods used to detect malicious node. The first sub-category considers end-to-end or hop-to-hop acknowledgements to directly locate the hops where packets are lost. A hop which has high packet loss will be removed from the route. The fourth sub-category considers the methods used in cryptography, for example bloom filter. But by these methods, selective packet dropping attacks are hard to identify.

The second sub-category uses the credit system discussed in [13] & [14]. A node receives credit by transmitting large number of packets to other nodes and uses that credit to send its own packets even if it is a malicious node. The node gains good credit by transmitting large number of packets and so it is hard to detect a malicious node if it makes a selective packet dropping. The second sub-category is the reputation system discussed in [15]. A reputation system depends on neighbor nodes to monitor and

IIOAB JOURNAL
ISSN: 0976-3104

identify misbehaving nodes. A node which highly drops the packet is given a bad reputation by its neighbor nodes. This information based on the reputation is sent periodically throughout the network and is used as an important factor in selecting routes which does not have malicious node. This method will be suitable only to detect blackhole attacks but not suitable to detect other types of attack. In [16], the author proposed an anomaly-based IDS system on an enhanced windowing method to carry out the collection and analysis of selective drop attack. This method leads to some miss calculation and detection accuracy. A Record and Trust-Based Detection (RTBD) technique was proposed in [17] which lead to low performance evaluation when the trust is created based on credit system. In [18] the author proposed an intrusion detection system which removes the fake nodes but does not contain any authentication method for privacy purpose. In [19], an approach that deals with routing misbehavior is discussed. The proposed approach can be integrated with any source routing protocol and detects malicious node based on sending acknowledgement packets and counting the number of data packets of active path. This method fails to detect the truthfulness of the node and lack of privacy.

After reviewing the above works, it is observed that some of the issues are not yet completely addressed. In existing systems, attack detection is limited to static or quasi-static wireless ad hoc networks. The existing credit based mechanism for the detection of selective packet dropping attacks may fail to detect the malicious nodes accurately. Reputation based approach is not so efficient in finding malicious nodes which drops the packets selectively and also truthfulness of the nodes are not detected. Hence, we propose an extended HLA signature approach to address the above issues and also for privacy preserving during auditing. We also enhance our work by increasing the auditor nodes to increase the detection accuracy. A new algorithm for creating the suspected node list is proposed to reduce the communication overhead.

Network model

In a wireless ad hoc network shown in Fig.1, consider a path $P_{SD,}$ where S is the source node and D is the destination node. Consider nodes n_1 , . . , n_k as the intermediate nodes. Therefore n_i is considered as the upstream node for n_{i+1}. If Dynamic Source Routing (DSR) protocol is used then it is considered that the source node is aware about the path P_{SD} or else trace route operation is used to identify the neighbour nodes being involved in the path. The symbols and their description that are used in the proposed scheme are given in [Table 1].

Table1: Symbols and Notations

Symbols	Description
S	Source node
D	Destination node
P_{SD}	Path from source to destination node
n_j	Numbers assigned to the nodes
H	Hash values
S_{ij}	Signature generated to the intermediate nodes
b_{ij}	Bitmap generated by each node
$r^{(i)}$	Linear combination
$S^{(j)}$	Signature combination
T_{ij}	Computed homomorphic linear authenticated key
P_D	Probability of packets received at destination node
T_{PL}	Packet loss threshold value
A_d	Auditor node
E	Equality testing
γ_j	Autocorrelation function calculated at auditor node

The wireless channel alternates between good and bad state at each hop for each random process. When the transmission of packet is successful then it considered to be good state [19] .If there is any loss in the packet transmission then it is in bad state. The sequences of packet transmission at each state is considered and based on that sequence autocorrelation function is used to detect the packet loss. The receiver observes the transmission and obtains the realization of the channel state (a_1, . . . , a_M), where $a_j \in \{0,1\}$ for j=1, . . , M. Here "1" states that packet was received successfully and "0" states that packet was dropped. There is another node which acts as an independent auditor A_d in the network. The auditor node is not a part of the path P_{SD}. It does not have any knowledge about the key and also about the content inside the transmitted packet.

[Fig.2] shows the overall process of the proposed system. The process is split into four phases. In the first phase, the process of key distribution is carried out. The packets are transmitted securely in the second phase. The auditing based on bitmap generated and detection of attack is carried out in third and fourth phase respectively. The source node distributes the symmetric keys to all nodes along with hash function. According to our proposed scheme, the packets are transmitted along with the signature for privacy preserving purpose. Hence the path is secured and privacy preserved. The packet transmission status is stored at the database of each node which is further used to generate a bitmap. The destination detects the occurrence of packet loss and intimates the source node. The source node verifies the intermediate nodes randomly and creates the suspect list. Then the source node sends the attack detection request to

IIOAB JOURNAL
ISSN: 0976-3104

the nearest auditor node. The auditor node verifies the bitmap of the suspected nodes and then calculates the autocorrelation function and detects the malicious node.

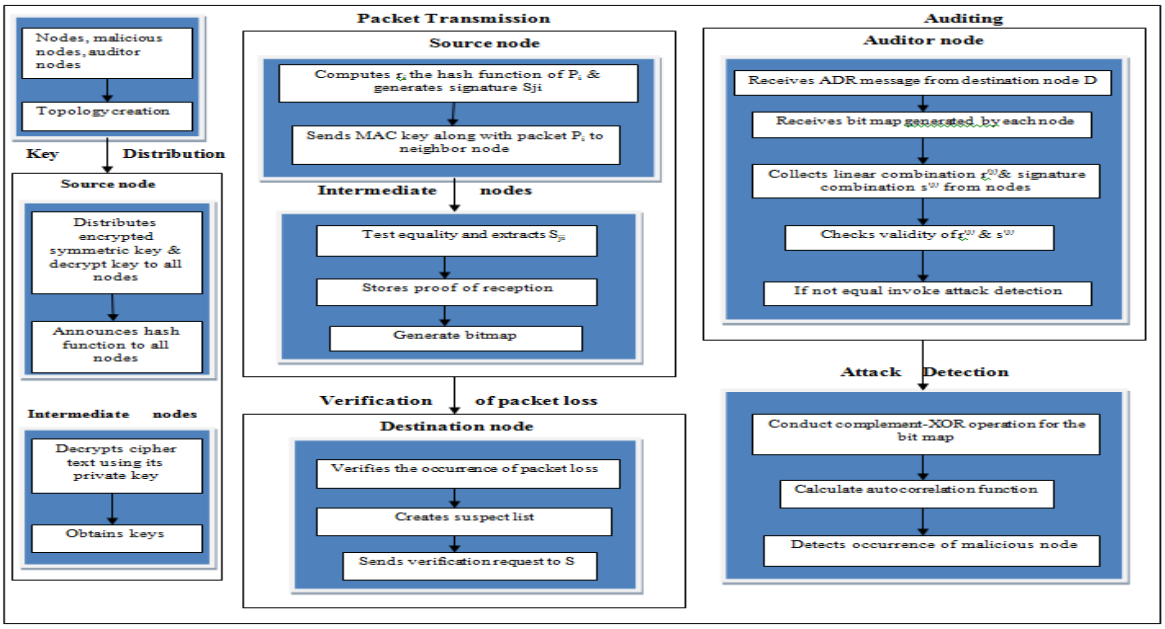

Fig.2: Functional Architecture

Key distribution

As we are using DSR routing protocol, we assume the path from source to destination as P_{SD}. The source node S makes decision on a symmetric-key crypto-system ($encrypt_{key}$, $decrypt_{key}$) and K symmetric keys $key_1, \ldots, key_k$. The source node distributes the decrypt key and a symmetric key key_j to its neighbor nodes n_j which exists in the path. RSA is used for key distribution. Using the public key of the intermediate nodes n_j where j=1 to k, the source node encrypts and sends the cipher text to n_j. After receiving the packet, the intermediate nodes decrypt the cipher text using its private key and extract the decrypt key and symmetric key key_j. The source node also announces two hash functions to all nodes in the path which can be used for authentication purpose.

Packet transmission

Source node S transmits the packet after the distribution of keys. S selects the packet P_i to be sent, where "i' is the sequence number assigned to packets to identify them uniquely. S computes r_i, the hash function of the packet P_i. The hash function of P_i is computed such as $r_i=H_1(P_i)$. S then generates an extended HLA signature for node n_j as shown in equation (1).

$$S_{ji}=[H_2(i||j)u^{r_i}]^x, \text{for } j=1,\ldots,k, \quad (1)$$

Here a one way chained encryption is used, it prevents an upstream node from deciphering the signature send to downstream nodes. By using this one way encryption, the S_{ji} is sent along with P_i. S also iteratively computes the following parameters as in equation (2).

$$\tilde{s}_{Ki} = encrypt_{keyK}(s_{Ki}),$$
$$\tau_{Ki}=\tilde{s}_{Ki}||MAC_{keyK}(\tilde{s}_{Ki}), \quad (2)$$
$$\vdots$$
$$\tau_{ji} = \tilde{s}_{ji}||MAC_{keyj}(\tilde{s}_{ji}),$$

Where Message Authentication Code (MAC) is computed according to the hash function H_{keyj}^{MAC}. S puts P_i and τ_{1i} in one packet and sends it to node n_1.n_1 receives the packet from S and extracts P_i and τ_i. Then n_1 verifies the integrity of $\tilde{s}_{1i}$ by testing the equality as shown in equation (3)

$$MAC_{key1}(\tilde{s}_{1i})=H_{key1}^{MAC}(\tilde{s}_{1i}). \quad (3)$$

If the result of the test is true, then n_1 decrypts $\tilde{s}_{1i}$ as shown in equation (4).

$$Decrypt_{key1}(\tilde{s}_{1i})=s_{1i}||\tau_{2i}. \quad (4)$$

If the test of equality fails, then n_1 stores loss of P_i in the proof of reception database. Once if the test is proved to be true then n1 stores r_i and s_{1i} in its proof of reception database. Each node after receiving the packet stores the data of reception in the database maintained by each node individually. The data is stored as FIFO manner. This proof is used for auditing later. Then n_1 puts P_i and τ_{2i} in one packet and transmitted to n_2. The above process is repeated at every intermediate node n_j. The last intermediate node n_k, only forwards P_i to the destination D.

IIOAB JOURNAL
ISSN: 0976-3104

Verification of Packet Loss

Here, we propose an algorithm for the verification of packet loss and for creating suspected node list. The destination node identifies that the actual number of packets it received from its previous hop node is less than the number of packets the source node sends and then sends packet loss message to source node. Then S starts the suspected node discovery process. First it sends a request to the intermediate nodes randomly. The intermediate nodes after receiving the request, send the number of packets they received and forwarded to the node S. Based on this count, the source node verifies at which node there is a change in the number of packets. The node which has varying number of packets received and its neighbor node is added to the suspected list. After creating the suspected list, the source node sends the attack detection request to the nearest auditor node [13].

We denote the number of packets forwarded by source node S to destination node D in a block be N_S. Let nodes a_0, a_1, a_2,a_3, . . . , a_n represent the source route or data forwarding route between source node S and destination node D. When the destination node receives the data packets from the source, it starts a counter and keeps count of number of data packets it receives in a block. Let N_D denotes the packets received at the destination node, and then the probability of packets received at the destination node is calculated as follows: $P_D = \frac{N_D}{N_S}$. If $P_D > T_{PL}$, then the destination node starts the process of detecting whether any malicious node is present in the route as shown in [Fig.3]. If not, then the destination node sends the positive acknowledgement back to the source node. Here T_{PL} represents the packet loss threshold value and takes values between 0 and 0.2. In our approach, the destination node starts the gray hole detection process, when the data packet loss exceed 20% of the total packets sent by the source node.

Algorithm:

if source node
Intimate to the destination, the count of data packets in a block of data
Send one block of data through the path selected through route discovery process
else if destination node
Compare the data packets received with the data count intimated by the source.
Calculate the probability of packets received at the destination node as P_D.
if $P_D < T_{PL}$ (the value of T_{PL} is between 0 and 0.2)
Send positive acknowledgement back to source node.
Else
Creates the suspected node list
Initiate Attack Discovery Process
end if

Fig.3: Pseudo code for verification of packet loss

Auditing method

In this section, an improved auditing method is discussed to enhance the attack detection accuracy. The source node sends the Attack Detection Request (ADR) message to a public auditor. This message contains the id of the nodes in the path P_{SD}. The identities are listed in the order of downstream direction. The auditor node is also provided with the information about sequence number of the packets sent from source node and also the sequence number of the subset of these packets that were received by destination node. Here, we use multiple auditing nodes. One auditing node is added to each two hops. Hence, auditing is done in an efficient way. All the auditing nodes precede the process in the same manner as follows. The auditor node submits a random challenge vector to each node in the path. At each node the sequence number of the packet received is stored in the database. Based on this proof of reception stored in the database, the bit map b_j is generated by node n_j. Here the $\vec{b_j}$ = (b_{j1}, . . . , b_{jM}) where b_{ji}=1 if the packet is received at that particular node and b_{ji}=0 if the packet is not received at the particular node. The linear combination $r^{(j)}$ and an extended HLA signature combination $s^{(j)}$ is calculated at node n_j, as in equation (5).

$$r^{(j)} = \sum_{i=1}^{M}, b_{ji}\neq 0\ c_{ji} r_i \ ,$$

$$s^{(j)}=\prod_{i=1, b_{ji}\neq 0} s_{ji}^{c_{ji}} \ . \qquad (5)$$

After calculating n_j submits $\vec{b_j}$, $r^{(j)}$ & $s^{(j)}$ to A_d. Then A_d checks the validity of $r^{(j)}$ & $s^{(j)}$ by testing the equality as in equation (6).

$$e(s^{(j)},g)=e(\prod_{i=1,b_{ji}\neq 0}^{M} H_2\ (i||j)^{c_{ji}} u^{r^{(j)}}, v) \qquad (6)$$

If the result of testing is true, then A_d accepts that node n_j received the packets as reflected in $\vec{b_j}$. If the testing results in false then A_d rejects $\vec{b_j}$ and judges that not all packets claimed in $\vec{b_j}$ are actually received by n_j. The above mechanism only guarantees that a node cannot understate its packet loss, i.e., it cannot claim the reception of a packet that it actually did not receive. This mechanism cannot prevent a node from overly stating its packet loss by claiming that it did not receive a packet that it actually received. This latter case is prevented by next phase called attack detection.

IIOAB JOURNAL
ISSN: 0976-3104

Attack detection

After receiving bit map and the auditing process, the auditor A_d enters the detection phase. A_d detects if there is any overstatement of packet loss at each node by constructing a packet loss bitmap for each hop. A_d checks the consistency of the bitmaps for any possible overstatement of packet losses. If there is no overstatement of packet loss, then the set of packets received at node j+1 should be a subset of the packets received at node j. A normal node always truthfully reports its packet reception bitmap. A malicious node will not truthfully report its packet reception bitmap. Hence bitmap of a malicious node will contradict with the bitmap of a normal downstream node. There will always be at least one downstream node i.e. destination node. So A_d only sequentially scans bitmap reported by intermediate node and the report from D to identify nodes that are overstating their packet losses. After checking for the consistency of bitmaps, A_d starts constructing the per-hop packet-loss bitmap $\vec{m_j}$ from $\vec{b_{j-1}}$ and $\vec{b_j}$. This is done sequentially, starting from the first hop from S. In each step, only packets that are lost in the current hop will be accounted for in m_j. The packets that were not received by the upstream node will be marked as "not lost" for the underlying hop. Denoting the "lost" packet by 0 and "not lost" by 1, $\vec{m_j}$ can be easily constructed by conducting a bit-wise complement-XOR operation of $\vec{b_{j-1}}$ and $\vec{b_j}$.

Next the auditor calculates the autocorrelation function γ_j for each sequence $\vec{m_j}$= (m_{j1}, . . ., m_{jM}), j=1, ...,K, as shown in equation (7):

$$\gamma_j(i)=\frac{\sum_{k=1}^{M-i} m_{jk}\ m_{jk+i}}{M-i} \quad (7)$$

After calculating the auto correlation function for each sequence the auditor calculates the relative difference between γ_j and the ACF of the wireless channel f_c as shown in equation (8).

$$\epsilon_j=\sum_{i=0}^{M-1}\frac{|\gamma_j(i)-f_c(i)|}{f_c(i)} \quad (8)$$

The relative difference is then used as the decision statistic to decide whether or not the packet loss over the jth hop is caused by malicious drops. In particular, if $\epsilon_j \geq \epsilon_{th}$, where ϵ_{th} is an error threshold, then A_d decides that there is malicious packet drop over the hop. Here we use the overhearing technique and trust based value evaluation to detect the malicious node in mobile nodes. By using the trust based method, the auditor node calculates the trust value for each node based on the packets it has transmitted. If the trust value goes above the threshold value then the auditor node decides that the node is a reason for malicious drop.

RESULTS

Security and overhead analysis

Our construction essentially follows the BLS-signature-based HLA construction for a given node n_j, as described in [2]. Under the implicitly assumed condition of no collusion between attackers, the authors in [2] proved that the construction is secure, i.e., here only the node which knows about an extended HLA signature can respond to the challenge. There is no possibility for the occurrence of forgery. So here even if there occurs the collusion between malicious nodes, the node does not give the attacker more information about the an extended HLA signature of the packets. We consider some properties of HLA signature to prove this,

1) For a packet P_i, an extended HLA signature is given as s_{ji}, here (i) is the sequence number assigned to the packet and (j) is the unique identity given to the node. This means that for the same packet, each hop on P_{SD} is given a different HLA signature. The verification scheme accounts for both i and j. In case there is no occurrence of collision, the security of the proposed scheme can be proved by concatenation of (i| |j) as a Meta packet sequence number.

2) As we are using the one way chained encryption the upstream node cannot get an extended HLA signature intended to the downstream node. As the one way encryption is used the upstream node cannot decrypt the packet send to downstream node. The downstream node can decrypt and get its extended HLA signature and send it to upstream node through a covert channel, if it is a malicious node. If the upstream node drops the packet then the downstream node has no other way to get its HLA signature. So if there is no collision, then more information about HLA cannot be exchanged by the covert channel.

Communication overhead

The communication overhead for the key distribution phase is a one-time cost that incurred when the routing path P_{SD} is established. Here we mainly focus on the cost during the packet transmission and auditing phases (there is no communication overhead in the detection phase). In the packet transmission phase, S sends one encrypted HLA signature and one MAC key along with the each packet it transmits. An extended HLA signature s_{ij} is of 160-bit long. The encryption process is of 192 bits in length. The hash function is of 160 bits. So each hop of packet transmitted is of 352 bits. In our proposed system, we create a suspect list and auditor node verifies only those nodes. Hence the communication overhead is reduced in our proposed system as shown in [Fig: 4].

IIOAB JOURNAL
ISSN: 0976-3104

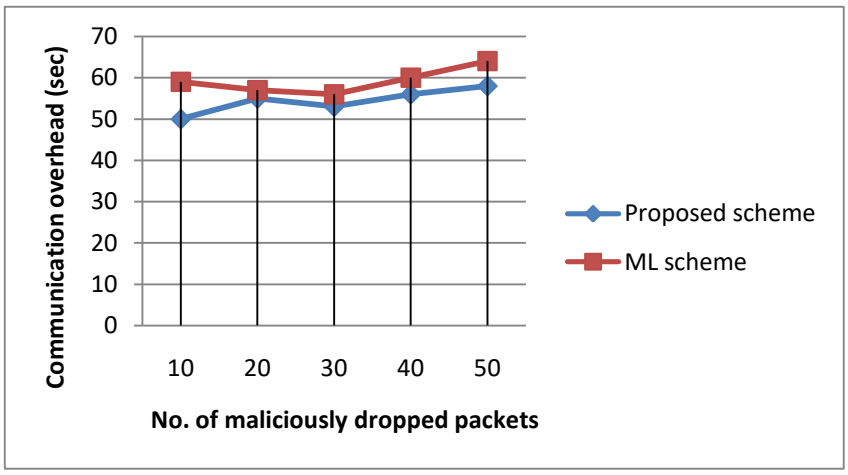

Fig.4: Communication overhead

Simulation setup

The proposed model is simulated using Network Simulator (NS) with its version 2.35. The required system parameters are configured using the TCL. The following [Table 2] represents the parameters used in the simulated environment. The proposed model is carried out with the simulation time 120s.

All the given parameters have to be set first. The nodes are placed at a position initially. Since client nodes are mobile they move in different direction. Due to this mobility of client routes will be changed frequently. To attain the MAC characteristics, here the 802.11 MAC protocol is used. The initial step of nodes displayed in NAM file is shown in [Table 2].

In this work, we compare the detection accuracy achieved by the proposed algorithm with the optimal maximum likelihood algorithm, which only utilizes the distribution of the number of lost packets. For given packet-loss bitmaps, the detection on different hops is conducted separately. So, we simulate the detection of one hop to evaluate the performance of a given algorithm. We also assume that packets are transmitted continuously over this hop, i.e., a saturated traffic environment. We assume channel fluctuations for this hop follow the Gilbert-Elliot model, with the transition probabilities from good to bad and from bad to good given by P_{GB} and P_{BG}, respectively [19]. We consider a selective dropping attack.

Table 2: Simulation parameters

Parameters	Value
Simulator	Network Simulator 2
Topology	Random
Interface type	Phy / wirelessPhy
MAC type	802.11
Queue type	Drop Tail/Priority Queue
Queue length	100 Packets
Antenna type	Omni Antenna
Propagation type	Two Ray Ground
Routing protocol	DSR
Application agent	Security
Network area	600*600
Number of nodes	70
Simulation time	120 seconds

As shown in the [[Fig.5], the overall detection error is less in the proposed system when compared to the earlier scheme known as Maximum Likelihood scheme (ML scheme) [20]. In the selective dropping attack, the packets dropped are of certain sequence numbers. During analysis, this is done by dropping the middle N of the M most recently received packets. In this work, we have considered in following three performance metrics: probability of false alarm (P_{fa}), probability of miss detection (P_{md}), and the overall detection-error probability (P_{error}). We collect these statistics as follows. In each run, we first simulate some independently generated packet-loss bitmaps for the hop, where packet losses are caused by link errors only. We execute our detection algorithm over these packet-loss bitmaps and collect the number of cases where the algorithm decides that an attacker is present. Let this number be I_{fa}. The probability of the false alarm of this run is calculated as false alarm of link error divided by the number of bitmaps generated. We then simulate another set of independently generated packet-loss bitmaps, where losses are now caused

IIOAB JOURNAL
ISSN: 0976-3104

by both link errors and malicious drops. Let the number of cases where the detection algorithm rules that an attacker is not present.

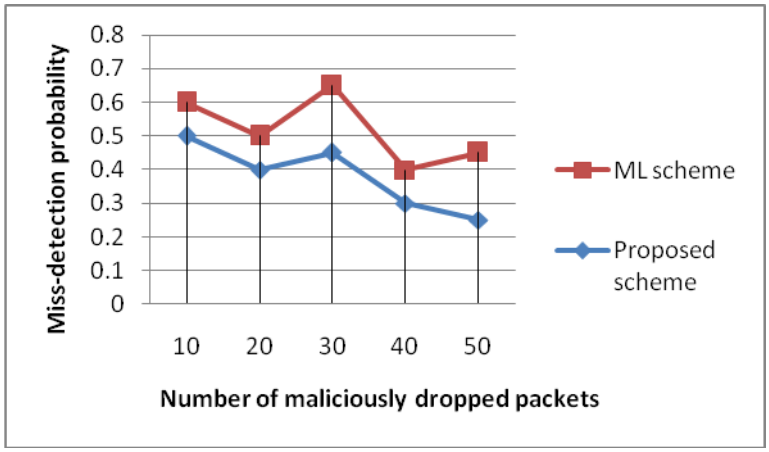

Fig.5: Miss-detection Probability

Probability of miss-detection (P_{md}) = $\frac{\text{verfication of attackers not present } (I_{md})}{\text{number of bitmaps generated}}$

[Fig.5] shows the probability of miss-detection by comparing the proposed scheme with the maximum-likelihood scheme. Sometimes it is considered that packet los is caused due to malicious node and link error is not considered. Hence this leads to miss-detection. Consider the simulation of 70 independently generated packet-loss bitmaps, where losses are now caused by both link errors and malicious drops. Let the number of cases where the detection algorithm verifies that an attacker is not present be I_{md}. P_{md} of the underlying run is given by $P_{md} = I_{md}/70$ [2].

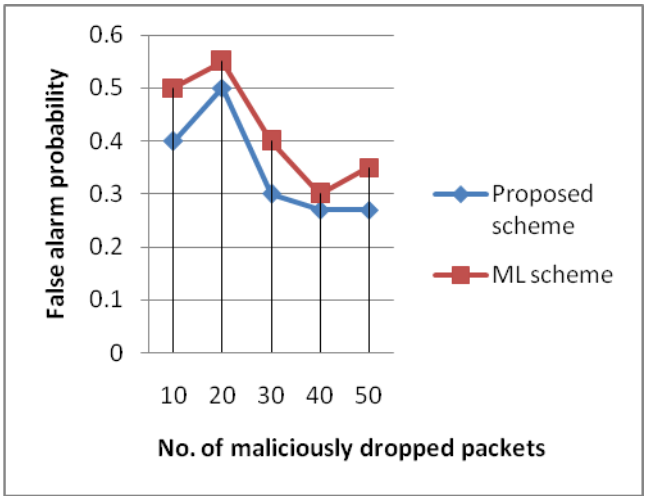

Fig.6: False-alarm Probability

Probability of false alarm (P_{fa}) = $\frac{input\ false\ alarm\ (I_{fa})}{number\ of\ packets\ sent}$

The probability of false alarm is that if any node which is assigned as attack node but not actually the attack node and hence the proposed scheme indicates the false alarm. [Fig.6] shows the probability of false alarm for increase in number of maliciously dropped packets by comparing the proposed scheme with the ML scheme. In each run, the simulation of 10 independently generated packet-loss bitmaps for the hop, where packet losses are caused by link errors only [19]. We execute our detection algorithm over these packet-loss bitmaps and collect the number of cases where the algorithm decides that an attacker is present. Let this number be I_{fa}. P_{fa} of this run is calculated as $P_{fa} = I_{fa}/100$.

ISSN: 0976-3104

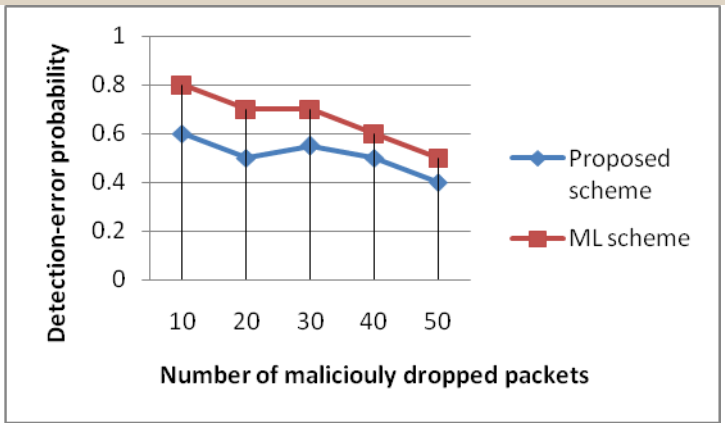

Fig.7: Overall detection-error probability

[Fig.7] shows the overall detection-error probability by comparing proposed scheme to the existing scheme. P_{error} is given by $P_{error}=I_{fa} + I_{md}/200$ [2]. The above simulation is repeated 30 times, and the mean and 95 percent confidence interval are computed for the various performance metrics.

CONCLUSION

In this work, the design and implementation of an efficient approach for privacy preserving and detection of selective packet dropping attacks in wireless ad hoc networks is discussed. The proposed scheme well preserves privacy during auditing by designing an extended HLA signature approach. An improved auditing method is designed to minimize communication overhead by increasing the number of auditor nodes and also to detect the truthfulness of the nodes. An algorithm for verification of packet loss is proposed for creating suspected node list which reduces the communication overhead. Selective packet dropping attack detection process for dynamic mobile environment is also discussed. The proposed design architecture is collusion proof, requires relatively high computational capacity at the source node, but incurs low communication and storage overheads over the route. The proposed mechanism also provides an increased accuracy in detection of malicious nodes and also shows low miss detection. The performance of the proposed system with respect to existing system is analysed and observed that there is increase in the detection accuracy based on the following metrics such as miss-detection probability, overall detection error and communication overhead.

In future, the detection mechanism can be carried out while the source and destination nodes are malicious nodes. The detection mechanism can be tested in various protocols and network environment to compare their performance. As a first step, this analysis mainly emphasize the fundamental features of the problem, such as the untruthfulness nature of the attackers, the privacy-preserving requirement for the auditing process, and the randomness of packet losses, but ignore the particular behavior of various protocols that may be used at different layers of the protocol stack. The implementation and optimization of the proposed mechanism under various particular protocols will be considered in our future studies.

CONFLICT OF INTEREST

The authors declare no conflict of interest.

ACKNOWLEDGEMENTS

None.

FINANCIAL DISCLOSURE

None

REFERENCES

[1] Aishwarya Sagar Anand Ukey and Meenu Chawla. [2010] Detection of Packet Dropping Attacks using improved Acknowledgement based scheme in MANET. IJCSI, 7(4):12-17.

[2] Tao Shu and Marwan Krunz. [2015] Privacy- Preserving and Truthful Detection of Packet Dropping Attacks in Wireless Ad hoc Networks. IEEE Transactions on Mobile Computing, 14(4):813-828.

[3] Bhavana V, Navamani TM. [2016] An Efficient approach for privacy preserving and Detection of packet dropping attacks in Wireless Ad hoc Networks. ICEECE conference.

[4] SenthilKumar Subramaniyan, William Johnson and Karthikeyan Subramaniyan. [2014] A Distributed framework for detecting selfish nodes in MANET using Record and Trust-Based Detection (RTBD) technique. EURASIP journal on wireless communications and networking, 1:1-10.

[5] Mohanapriya M and Ilango Krishnamurthi. [2013] Modified DSR protocol for detection and removal of selective black hole attack in MANET. Elsevie 40:530-538.

[6] Debdutta Barman Roy and Ritu Parna Chaki. [2011]MADSN: Mobile Agent based Detection of Selfish

IIOAB JOURNAL
ISSN: 0976-3104

Nodes in MANET. International journal of Wireless Mobile Networks 5(4):225-235.

[7] Alejandro Proano and Loulas Lazos. [2011] Packet-Hiding Methods for Preventing Selective Jamming Attacks. IEEE Transactions on dependable and secure computing 9(1):101-114.

[8] G Rajarajan and L. Ganesan. [2016] A Hybrid Approach to Protect Network Components from Distributed Denial of Service Attacks. Advances in Natural and Applied Sciences 10(1):117-122.

[9] Lilly Roseline Mary J and Buvana M. [2016] Secure and Efficient Data Gathering Using Trust Management Scheme and Intrusion Detection System in Wireless Sensor Network. Advances in Natural and Applied Sciences 10(1):123-129.

[10] Nilesh N. Dangare and RS Mangrulkar. [2016] Design and Implementation of Trust Based Approach to Mitigate Various Attacks in Mobile Ad hoc Network. Elsevier, 78:342-349.

[11] Aravind Dhaka, Amit Nandal and Raghuveer S.Dhaka. [2015] Grayhole and Blackhole Attack Identification using Control Packets in MANETS. Elsevier 54:83-91.

[12] Ashish Kumar, Vidya Kadam, Subodh Kumar and Shital Pawar. [2011] An Acknowledgement-Based Approach for the Detection of Routing Misbehaviour in MANETS. International Journal of Advances in Embedded Systems 1(1):04-06.

[13] Ateniese,G S. Kamara, and Katz.J. [2009] Proofs of storage from homomorphic identification protocols. in Proc. Int. Conf. Theory Appl.Cryptol Inf Security,319–333.

[14] Awerbuch B, R Curtmola, Holmer D, Nita-Rotaru C, and Rubens H. [2008] ODSBR: An on-demand secure byzantine resilient routing protocol for wireless ad hoc networks. ACM Trans. Inform.Syst. Security, 10(4):1–35.

[15] W.Galuba P. Papadimitratos, M. Poturalski, K. Aberer, Z.Despotovic, and W. Kellerer. [2010] Castor: Scalable secure routing for ad hoc networks. Proc. IEEE INFOCOM, pp. 1 –9.

[16] Leovigildo Sanchez-casado, Gabriel Macia-Fernandez. [2015] A model of data forwarding in MANETs for lightweight detection of malicious packet dropping. Elsevier in computer networks, 87:44-58.

[17] Proano.A and Lazos.L. [2010] Selective jamming attacks in wireless networks. proc. IEEE ICC Conf, pp.1-6.

[18] Devi Iswarya,G, V.lakshmipriya, M.Senthil and A.Kumaresan. [2016] Detection Of Isolation Attack Using Olsr Protocol On Manet. Advances in Natural and Applied Sciences, 10(5):97-101.

[19] Muhammad Imrana, Farrukh Aslam Khanb, Tauseef Jamala and Muhammad Hanif Durada. [2015] Analysis of Detection Features for Wormhole Attacks in MANETs. Elsevier Computer Science, 56:384 – 390.

[20] Snehal P. Dongarea and Prof. RS Mangrulkarb. [2016] Optimal Cluster Head Selection Based Energy Efficient Technique for Defending against Gray Hole and Black Hole Attacks in Wireless Sensor Networks. Elsevier, 78:423-430.