Detection of Impersonation Attack in MANET Using Polynomial Reduction Algorithm

Perumal Raghavan Kavitha, Rajeswari Mukesh
(Corresponding author: P. Kavitha)

Department of Computer Science and Engineering, Hindustan Institute of Technology and Science
Padur, Chennai, Tamil Nadu, India
(Email: kavithashree2007@gmail.com)
(Received Mar. 15, 2017; revised and accepted June 25, 2017)

Abstract

Secure routing among multiple routers become a complex process in Mobile Ad-hoc NETworks (MANETs) due to the presence of adversary nodes. An adversary node which compromises the honest node as well as it will use all secrets of compromised node. By these capabilities, the attacker launches impersonation attacks against secure transmission. Strengthening the personal key and monitoring the behavior of each node is crucial avoid impersonation attack. This paper proposed the Enhancing Polynomial reduction algorithm for Secure routing against Impersonation in Clustered MANET to tackle above secure routing issues. To provide the personal key with less key storage overhead, the clusters network based on the flexible weight clustering algorithm. To avert impersonation, the polynomial reduction algorithm which initially exploits the strong key authentication via two separate transactions which forward the set of primitive polynomial with key function and the same with anyone random number in a successive manner. Also, the polynomial reduction algorithm considers the acknowledgments with attached hop-counts from the intermediate routers to identify the impersonation when the attacker acts as an intermediate router resulting in high control overhead. Therefore, the proposed introduces the Energy Efficient Polynomial Reduction (EPR) algorithm that reduces the overhead by sending the consolidated acknowledgment for same cluster nodes.

Keywords: Clustering; Impersonation Attack; MANET; Polynomial Reduction Algorithm

1 Introduction

A collection of mobile nodes forms a self-configuring and temporary network using wireless links, named as Mobile Ad-hoc NETwork (MANET). The highly dynamic nature of MANET suffers the direct wireless communication due to the limited bandwidth and transmission range. For using multi-hop routing strategies, it is necessary to establish the wireless communication among remote mobile nodes [18]. Due to multiple intermediate routers in multi-hop routing, a secure packet transmission is not assured in the presence of impersonation attacks. In that attack compromises the legitimate node to launch some attacks against secure routing. The key authentication technique ensures a secure forwarding among multiple intermediate routers. The personal key authentication technique supports to avoid the impersonation. A private key is hacked by overhearing then node is stored, which leads to the possibility of launching impersonation attack [3, 12]. Furthermore, the key storage overhead and personal key maintenance escalate in each node in the group. Therefore, to ensure secure routing, it is necessary to consider the impact of impersonation with considerable overhead.

The standard works estimate the impersonation by employing a polynomial reduction method [7, 16]. The polynomial reduction algorithm identifies the impersonation according to the primitive and checks polynomials. However, the wireless medium gives the possibilities to overhear the key authentication. Thus, the attacker may trace the key through overhearing and initiate the false routing. Moreover, also this algorithm verifies the intermediate routers in the path by receiving the acknowledgments. Thus, it makes the high control overhead and network traffic. To tackle these issues, the Providing Enhanced Polynomial reduction algorithm for Secure routing against Impersonation in Clustered MANET is proposed to augment the key authentication methodology and identify the impersonation using Energy efficient Polynomial Reduction (EPR) algorithm with reduced routing overhead.

The significant strategies which contributions of the paper are as follows:

- The proposed protocol assures secure and reliable routing in the highly dynamic network by detecting and isolating the impersonation attacker in the routing path using EPR algorithm.

- By partitioning the network into several clusters using a weight clustering algorithm, and maintaining the cluster group key and separate personal key for authentication, restricts the nodes to initiate the malicious routing attacks with considerable key storage overhead.

- By forwarding the primitive polynomial set with key function and the same random number via two separate transaction steps in a successive manner to improve authentication.

- By generating the consolidated acknowledgment for the same nodes using group ID verification of previous and next-hop nodes, the protocol significantly lowers the acknowledgment overhead as well as escalates the energy storage.

Next section focuses exclusive study on MANET security routing protocols, Section 3 represents the problem statement, Section 4 shows System and Attack Model in MANET; Section 5 gives the overview of Proposed EPR (PEPR) protocol; Section 6 gives detailed performance evaluation for PEPR. and final section concludes the paper.

2 Related Works

Even though the routing protocol establishes the multihop routing using multiple intermediate routers, the secure and reliable data delivery is unlikely achieved if any impersonation attacker is selected as an intermediate router. The impersonation attacks target the data transmission functionality between source and destination. The adversary nodes compromise the genuine node to simply launch impersonation, dropping, and modification of the original data content to reduce the network performance. Several secure routing approaches have been proposed against such attackers in MANET [6, 8, 24].

The asymmetric group key provides the security with the public and private key. In this, the digital signature and data encryption are performed using the public key. The individual decryption key is maintained as confidential [25, 27]. Furthermore, the dropping attackers drop the received packets, either for saving their resources or for deliberately disrupting regular communications [9]. Observing the routing behavior of nodes is important to combat with a different variety of dropping attacks such as black-hole, gray-hole, and wormhole attacks [14, 20]. Such attacks drop the packets entirely or selectively. This kind of attackers can be identified by continuously monitoring the behavior of nodes during data forwarding. For example, the sender node can trace the data forwarding records of a particular packet at each node by formulating a Renyi-Ulam game based tracing. In this, the first hop data packet forwarded is no longer considered as a misbehaving node [17]. The detection of packet dropping is accounted in the presence of link error and collision using the correlation between them. The correlation enhances the accuracy of drop detection with Homomorphic Linear Authenticator (HLA) based public auditing architecture. The HLA ensures the effectiveness of a packet loss report that is delivered by individual nodes [21]. Similarly, counting the number of lost packets caused by link error can assist to detect malicious packet dropper [13, 26]. Moreover, the clustered network handles the routing issues on routing and the cluster partitions efficiently identify the malicious node. The highly efficient node is selected as a CH for providing the secure communication via cooperative nodes [5, 19].

To support the secure routing, it is essential to consider both the dropping and modification attacks to maintain reliability and confidentiality without modification using cryptography based encryption method [11]. Several cryptography based routing protocols have been proposed for secure data forwarding [6]. The Advanced Encryption Standard (AES)-based routing algorithm helps to consolidate the data integrity using hash codes containing the data packets. The AES employed with Triple Data Encryption Standard (TDES) assist in preventing the Packet Dropping and Message Tampering Attacks [23]. The polynomial scheme supports the detection of attacker nodes. In [16], the clustering provided additional security and secured key transmission between Cluster Head (CH) and members. The soft computing assists in detecting the irregularity and misuse. In [22], the same group based key transmission is exploited to assure the secure routing. The Logical Key Hierarchy (LKH) is employed to accomplish the personal key refreshment. The Hop Count Based Key Selection (HBKS) technique uses symmetric key based authentication and key pre-distribution method to find the impersonation, dropping, and modification attackers. This method can only identify the attacker who is acting as an intermediate router, and it is not supported to prevent the attacker who serves as a source or destination. When the modification attacker performs quite brilliantly, identification of modification attack becomes more difficult due to the possibility of changes in the original message [1]. The asymmetric encryption reduces the key distribution burden using a pair of keys rather than a symmetric encryption method [15]. For example, the Optimized Link State Routing Secured by Dynamics key (OLSR-SDK) [10] protocol exploits the asymmetric key distribution. It deploys the dynamic keys and secures the traffic routing without degradation of network performance. The Radio Aware Optimized Link State Routing (RA-OLSR) protocol applies high-level security mechanism based on Identity-Based Encryption (IBE) which eliminates the need of verifying the public key authenticity [4].

3 Problem Statement

The secure routing is mainly depending on the key authentication and the group key as well as personal key

maintenance on each node that increases the key storage overhead. The conventional methods exploit the direct key transaction method. The main limitation of the wireless network is that other nodes can overhear the communication between any two nodes. This hole provides the chance for the impersonation attacker to hack the key transaction via overhearing, if it happens, the attackers impersonate the honest nodes which launch the severe malicious attacks on the routing using that traced personal key. The polynomial reduction algorithm aids to recognize the impersonation attack. Even though, it becomes complex when the credential information is hacked. To deal with this, the strong key authentication process is essential. Also, the conventional polynomial reduction methodology escalates the acknowledgment overhead and energy degradation even it can identify the impersonation attack it attacks on the current routing path may involve in the upcoming routing process due to lack of the attacker isolation. Hence, it is essential to forward the packets in a secure and reliable manner using exact impersonation attacker identification and attacker node isolation.

4 System and Attack Model

The network area of MANET is represented as $G(V, E)$ in which V represents a set of mobile nodes and E represents the direct communication links between two mobile nodes V. Transmission range of each node is represented as R. The nodes V can impersonate the legitimate nodes that launch some attacks against secure transmission. In a flexible weight clustering, network, $G|\{C^i, C^{i+1}, C^{i+2}, \cdots, C^{i+n}\}$ and (CH^i, CM^N) C^i; $(N = 1, 2, \cdots)$. The CH^i and CM^N exchange the key via separate two transaction steps to avoid the key transaction overhearing. Thus, the CM^N can initiate the routing without any impact of impersonation. The CH^i authenticates and verifies the CM^N uses a set of primitive and checks polynomials. The set of primitive polynomial contains $f(a, b, c)$, in this, a and b are the generalized components and c is the specific report which is generated based on the generalized components. The $f(a, b, c)$ and $f(a, b, c, R)$ are forwarded in separate successive manner. R is the random number. The PEPR has implemented the EPR algorithm for predicting the impersonation with reasonable overhead. In this, S sends $\{Encrypt(data), X^{h-n}\ (n = 0, \cdots, h)\}$ to its next-hop and the intermediate routers forward it until reaching the D. Each hop-router replies the S by sending the ACK with deducted hop-counts $(X^{h-1}, X^{h-2}, X^{h-3}, \cdots, X^{h-h})$. If more than one node C^i, sends the consolidated ACK to S, S identifies the impact of impersonation from the received ACKs. The identified attackers are isolated from the network performance by calculating RTT values of each router and hypothesis of other nodes. Assume the model that adversary can overhear the key transaction and impersonate the legitimate node to intercept the communication when it hacks the personal key of the nodes.

5 Overview of Proposed EPR Protocol

The most destructive attack in MANET is impersonation attack. The cluster based group key management which reduces the overhead. However, it has the possibility to track the confidential communication between nodes.In this, the confidential message can be decrypted by all the nodes in the same group using the same cluster key. Also, if the individual personal key of any node is tracked by an attacker, it can launch the impersonation attack in routing performance. Instead, two separate transactions based individual personal key sharing is a feasible technique to ensure the secure routing against such attackers in MANET.

The CH is responsible for providing the individual personal keys to all the nodes in the same cluster. In this, the separate personal key is given to the member nodes by CH via successive transactions, instead of directly exchanging the personal key. The incorporated value of both the set of a primitive polynomial and the same set with a random number are forwarded in two transactions that creates the confusion on exact key function overhearing. Thus, it can reduce the possibility of tracking the personal key exchange regarding overhearing. Additionally, in polynomial reduction, the overhead and energy are taken into account for improving the routing performance. When more than one node in the same cluster acts as intermediate routers, the Energy efficient Polynomial Reduction (EPR) algorithm reduces the overhead by sending the single consolidated acknowledgment instead of individual acknowledgment

5.1 Enhancing Security in Clustered MANET

The conventional routing methods propose cryptography based key encryption using public and private keys for reducing impersonation attacks in MANET. In case, the private key of a node is leaked, the impersonation attacker may throw the security issues by compromising the legitimate node. Moreover, the key maintenance of each node escalates the storage overhead. To maintain the trade-off between security and key storage overhead, cluster based key distribution model is exploited. To get away from frequent key refreshment for the entire network, the rekeying process is applied only to clusters. The secure routing depends on the key management, and also depends on the network parameter such as energy. Therefore, the flexible weight clustering approach is proposed to play a vital role in providing the energy efficient, secure routing.

The flexible weight clustering method allows the network partitions into groups of entities called clusters. Each cluster has a Cluster Head (CH) and cluster members who are in one-hop communication from CH. It is elected based on the combination of metrics such as mobility, density, energy, connectivity, distance, and many

other metrics. Each node in the cluster observes the routing metrics of its neighbor nodes using broadcast messages. Commonly, the node which has high connectivity and high battery power that has announced as a CH to its neighbors is shown in Equation (1), because such nodes are favorable to the accurate and energy efficient routing in a dynamic network.

In this, each node calculates the cluster score to itself and its neighbors for selecting CH based on connectivity, and battery power. The node which has a high cluster score compared with others announces it as a CH to its neighbors. If a node receives CH announcement from more than one CHs, it chooses any one of the CH depending on its convenience. The node selects one CH with large cluster score, and it joins as a member under the selected CH.

$$N_{(CH)value} = (a \times \frac{N_{\mathrm{Co}}}{N_{\mathrm{Cmax}}}) + (b \times \frac{B_i - B_c}{B_i}). \quad (1)$$

Where $N_{(CH)value}$ represents the clustering score of each node, N_{Co} and N_{Cmax} represent the original connectivity (number of neighbors) and maximum connectivity of nodes in the network area respectively. B_i is the initial battery power, and B_c is a consumed power. The maximum connectivity is calculatedusing Equation (2). Where, v is the number of nodes in a particular area (HW).

$$N_{\mathrm{Cmax}} = \left[\frac{v}{H \times W}\right] \times R^2 \quad (2)$$

$$(a + b) = 1. \quad (3)$$

a and b are the weighting factors of connectivity and energy parameters respectively. It can weigh the parameters to obtain the estimated quantity. The sum of the weighting factors is shown in Equation (3). Algorithm 1 shows the flexible weight clustering algorithm.

Moreover, CH is appointed in a rotating manner, which means the same node does not elect as a CH continuously. The CH role rotation among real nodes balances the energy consumption among them. The nodes in the cluster cannot involve in any routing performance without having the acknowledgment from its CH. The CH supports the cluster and personal key refreshment and thus, it can avoid the member nodes to launch the impersonation attack using multiple transactions based key authentication in most of the cases.

Algorithm 1 Flexible Weight Clustering Algorithm

```
Aim: To partition the network into clusters
Input: CH score value of each node
Output: Election of CH and members
Begin
Each node do {
Calculates its own connectivity based on the number of neighbors (Nc);
Calculates the remaining energy level (Ne) based on their initial energy and consumed energy;
Estimates the CH score value according to both Nc and Ne;
Shares their own CH score value to their neighbors;
Compares their own value with other's value;
}
A node N_i that has the high CH score than others broadcasts the CH announcement;
The other nodes that has CH score<Score of N_i forward the reply to N_i to join as a member under N_i;
If (Received CH announcement == 1)
    { Node joins under that CH node; }
else (Received CH announcement > 1)
    {Node selects any one CH announcement based on its convenience;
    Node forward the reply to join as a member under the preferred CH;
    }
The Selected CH starts the authentication key sharing process between its members;
End
```

6 Avoiding Impersonation Using Energy Efficient Polynomial Reduction Algorithm

The polynomial reduction algorithms identify the impact of impersonation in the routing path. In the clustered network, the CH is responsible for distributing the separate personal key to their members. In this, all nodes in the cluster are enabled to maintain the set of a primitive polynomial which contains two generalized components and one specific report. This can be generated by using other two generalized components, which is observable by everyone due to the nature of the wireless medium. By this hole, an attacker can overhear and generate the same specific report as the similar report of the honest node using that generalized component. Thus, the CH mistakenly authorizes the attacker as a legitimate node and provide the key to an attacker resulting in impersonation attack launch. To strengthen the key authentication, the polynomial reduction algorithm initially exploits the two steps in the authentication process with the help of any random number support.

6.1 Step 1: Strengthening the Key Authentication

The polynomial reduction algorithm initializes all mobile nodes and the network with $f(a, b, c)$. In this, a, b, c represents the node ID, all forwarding nodes ID, and all measurement reports respectively. Function a and b are the generalized components and c is the specific report which is based on a and b. The c report is encrypted using the cluster key and stored in that node. The CH knows the node ID as well as the primitive polynomial set of all members. The authentication polynomial is computed for

cluster 'Cx' as follows:

$$Auth_x^p(b,c) = \alpha f_x(p,b,c).$$

Where, $f(nodeID,b,c)$ represents the set of primitive polynomial. $\{2, 2^2, 2^3, 2^4, 2^5\}$. Note that the algorithm randomly chooses the value α while computing the authentication polynomial. The algorithm only knows the value of α. Otherwise, no other persons can extrapolate the authentication polynomial of cluster 'Cx'. The purpose of α is to escalate the flexibility of this scheme on the number of compromised nodes. After the computation, the $Auth_x^p(b,c)$ is stored in node 'p'. Subsequently, the algorithm computes the verification polynomial as follows. For each cluster, (x,y).

$$Verf_y^p(a,c) = \beta f_y(a,p,c).$$

Where, $Verf_y^p(a,c)$ is the verification polynomial of cluster 'Cy' and it is stored in node 'p'. In this, $\{2^5, 2^6, 2^7, 2^8\}$, it performs the same role as, and in such 2^t, t is the positive integer. Both the value of α and β is taken into verification using check polynomial β/α. The value of β/α only belongs to the $\{2^0, 2^1, 2^2, 2^3, 2^4, 2^5, 2^6, 2^7\}$. For example, $2^5/2^5 = 2^0 \cdots 2^8/2 = 2^7$. However, the hole in the polynomial reduction is the report may be generated as equal to the legitimate node by an attacker using the generalized components that lead to the mistake verification. To overcome this, the proposed method exploits the two-step authentication. In this, the incorporated function value of a, b, c and ab, c, rare forwarded in the separate and successive manner via two transactions. R is the random number selected by the node. The both are forwarded in an unpredictable manner that means the $f(a,b,c)$ may send either firstly or secondly as the same the $f(a,b,c,R)$ may send in either firstly or secondly. The random number creates the confusion on the attacker decision about which is the original report. It strongly assists the polynomial reduction algorithm to correctly verify and distribute the key to the legitimate node without the impact of any impersonation. Algorithm 2 shows the separate function transaction algorithm via two steps.

In the above algorithm, the CH authenticates and verifies the node only after receiving the two function values from the same node to avoid the impersonation. Now, both the node and the CH know the report 'c' and creates the key. The node exploits the generated key to encrypt the data during forwarding.

Algorithm 2 Separate Function Transaction Algorithm

1: Aim: To restrict the impersonation as original
2: Input: The set of primitive polynomial and the random number
3: Output: Original report identification and verification
4: Begin
5: CH Sends the request to CM^N in cluster C ($N = 1, 2, \cdots, n$);
6: CM^N select the random number R;
7: CM^N incorporate the random number with $f(a,b,c)$ and generate another $f(a,b,c,R)$;
8: CM^N forward the two separate functions in two forwarding steps to the CH;
9: CH receives one function and wait for some time to receive the another function value;
10: After receiving the both $f(a,b,c)$ and $f(a,b,c,R)$, the CH verifies the CM^N;
11: CH splits the report 'c' and 'R' from both received values;
12: CH generate the original report based on its own primitive polynomial set for that CM^N;
13: CH compares the report computed by itself with the node report using check polynomials;
14: If (Report == same)
15: { The CH generates the key for that corresponding CM^N; }
16: else
17: { The CH identifies the attacker and discards the report; }
18: End

6.2 Step 2: Energy Efficient Polynomial Reduction Algorithm

Strengthening the Key Authentication ensures the nodes to initiate the secure forwarding without any impact of impersonation. In case, the routers misbehave in the discovered shortest routing path based on AODV, which severely makes the routing performance. To overcome these issues, the polynomial reduction algorithm efficiently finds the router impersonation using received acknowledgments with reduced hop-counts (X^h, X^{h-1}, X^{h-2}, X^{h-3}, $\cdots$, X^{h-h}). Every intermediate node sends back the acknowledgment to the sender node that ensures the successful data forwarding in hop-by-hop. However, when the number of acknowledgment escalates on the forwarded data packets, it results in high energy consumption. To tackle this inconvenience, in addition to the security, the proposed method considers both the acknowledgment overhead and energy that is named as the Energy efficient Polynomial Reduction (EPR) algorithm.

The possibility of presenting more than one router in the same cluster is high due to the distributed structure of the MANET. The high possibility reduces the chances of generating the individual acknowledgments in the same cluster. Thus, the consolidated acknowledgment escalates the advantages of improving both the overhead and energy consumption. For example, the representation of EPR algorithm is shown Figure 1.

In Figure 1, S forwards the data packets and estimated remaining hop-count X^4 to the intermediate Router 1 in C2. The Router 1 checks its group list, and it finds the position of Router 2 which is in other cluster C3. The Router 1 in C2 sends the acknowledgment ($X^{4-1} = X^3$) to S (source) after forwarding the data packets to Router 2.

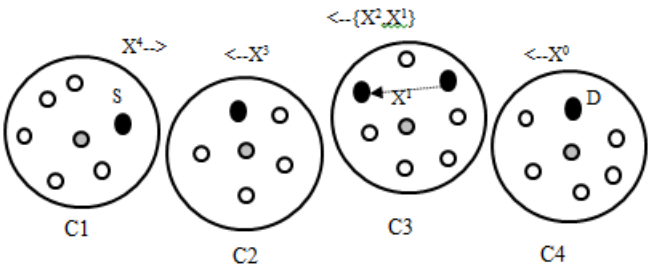

Figure 1: Representation of EPR algorithm

Router 2 in C3 forwards the packet to router3 and the Router 2 identifies the position of router3 by verifying group list. Therefore, it waits for receiving the acknowledgment from router3. After receiving X^1 from router3, the Router 2 creates the consolidated acknowledgment using its $X^{4-2} = X^2$ and $X^{4-3} = X^1$. The consolidated $\{X^2, X^1\}$ is forwarded to S by the Router 2. Finally, the corresponding D sends its acknowledgment $X^{4-4} = X^0$ to S.

The sender node estimates the number of acknowledgments on the number of data packets sent and hop-count between itself and destination that means each hop router forwards one acknowledgment for each data packet. However, due to the acknowledgment consolidation of the proposed method, the number of received acknowledgments may differ from the estimated one. The number of unreceived acknowledgments is predicted using Equation (4).

$$ACK_{(unreceived)} = (P_i \times H) - \sum_{R_{n=1}}^{R_{n=D}} (ACK_{(sent)}). \quad (4)$$

Where, P_i represents the number of packets and H represents the expected hop-count between sender and destination. Rn indicates the intermediate routers and $(ACK_{(sent)})$ represents the number of acknowledgments sent by each intermediate router. In addition to the destination, every intermediate node is enabled to send an acknowledgment to the sender after transmitting the received packets. Even when the intermediate node increases the proposed methodology can identify the attackers successfully. The unreceived acknowledgments may be affected by impersonation attack, or it may be consolidated with other nodes acknowledgment. There is a need to differentiate from each other to exactly calculate the presence of malicious impersonation attackers using Equation (5).

$$Imp^H = ACK_{(unreceived)} - N^H_{(ACK(cons))}. \quad (5)$$

Where $N^H_{(ACK(cons))}$ represents the number of hops included in consolidated acknowledgment. The Imp^H implies the presence of impersonation attackers in a path. Algorithm 3 shows the proposed EPR algorithm.

Algorithm 3 The Proposed EPR Algorithm

1: Aim: To successfully predict the impersonation attacker in the routing path
2: Input: Key authentication and ACKs
3: Output: Successfully avoid the impersonation
4: Begin
5: Step 1. $Auth^p_x(b,c) = f_x(p,b,c)$. Authentication polynomial of cluster Cx for p;
6: Step 2. $Verf^p_y(a,c) = f_y(a,p,c)$. Computes and stores the check polynomial in node p; K_{c_x} is the cluster key of C_x stored in node p1;For each cluster x is not equal to y;
7: Step 3. $CH_x \rightarrow p : (p|CH_x)$. CH sends the local ID assignment request to each node in CH_x
8: Step 4. $P \rightarrow CH_x$: $(f(a,b,c),\ f(a,b,c,R))$. c is the specific report based on the generalized components (a,b) that is encrypted by K_{c_x} and R is the random number selected by node p.
9: Step 5. $c = H((Ea,b)K_{C_x})$. CH_x receives two function values; Calculates the specific report 'c' using its set of primitive polynomial for node p.
10: Step 6. CH_x verifies the report c using check polynomials and get the key.
11: Step 7. c of $CH_x = c$ of p. The report that is generated by cluster head and node is same, the CH_x authorizes the node p; The node p encrypts the data using k_{c_x}.
12: Step 8. The node p identify the impersonation among intermediate routers using received ACK with attached hop-counts.
13: I. $p \rightarrow R_n$: $[E(Mesg), X^h)]$. The source node sends the data packet that contains encrypted message by its personal key and expected hop-count (X^h) to reach the destination.
14: II. $R_n \rightarrow R_n + 1$: $[(E(Mesg), X^{h-1}]$.
15: III. R_n checks the group list to know the current position of the next-hop router $(R_n + 1)$;
16: IV. If $(R_n + 1C_i)$, $R_n \rightarrow p : [X^{h-1}]$. C represents same cluster. Next-hop router is not located in C, R_n forwards the ACK to p.
17: V. If $(R_n + 1C)$,
18: Begin
19: R_n wait for some time to receive the acknowledgment from $R_n + 1$;
20: $R_n + 1$ checks the group list to identify the ID of its previous-hop (Rn) whether it is in the same group ID or not. If yes, follows Step 6;
21: VI. $R_n + 1 \rightarrow R_n : [X^{h-2}]$. After some time (viz $R_n+1 \rightarrow R_n+2 : [(E(Mesg), X^{h-2})])R_n+1$ forwards acknowledgment to R_n.
22: VII. $R_n \rightarrow p : [\{X^{h-1}, X^{h-2}\}]$. R_n forwards the consolidated acknowledgment to p;
23: The intermediate routers follow the above steps from II to VII until reach the destination (D) that means $D \rightarrow p : [X^{h-h}]$. }
24: End

7 Performance Evaluation

The extensive NS2 simulation is applied to validate the performance of proposed EPR Algorithm (PEPR) with the existing Polynomial Reduction Algorithm (ExPRA) [2]. The simulation takes 30, 100 and 200 mobile nodes over an area of 500m x 500m, 1000m x 1000m, 1500m x 1500m. The transmission range of each mobile node is 250m. The overall simulation time is taken of 60 seconds. The proposed method ensures the identification and detection of impersonation attacker with less overhead. The two-step exchange process of primitive polynomial set assists to generate the confusion on attacker overhearing. This process enables the member nodes to share their personal keys with CH in a secret manner. The acknowledgment consolidation for same cluster nodes leads to attaining low overhead. The proposed proves the performance through the detection accuracy, when compared to ExPRA with varying number of attackers.

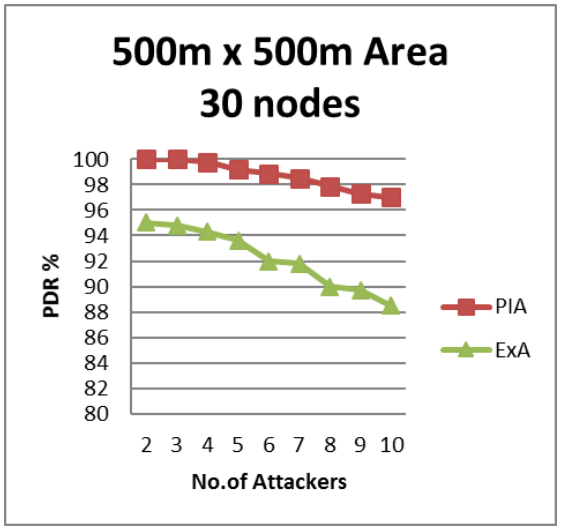

Figure 2: Detection accuracy vs number of attackers for 30 nodes

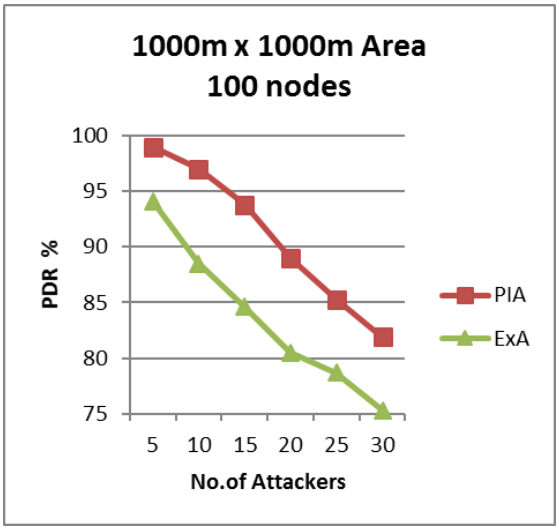

Figure 3: Detection accuracy vs number of attackers for 100 nodes

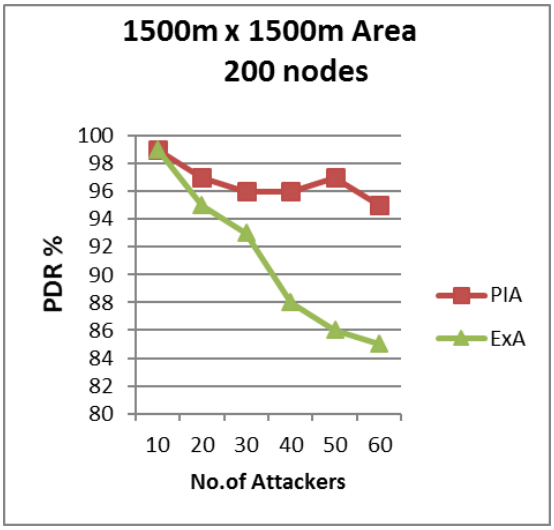

Figure 4: Detection accuracy vs number of attackers for 200 nodes

Figures 2, 3, 4 exposes the attacker detection accuracy of both the proposed EPR and ExPRA with varying number of attackers. Initially, the PEPR has 100 % detection accuracy compared to ExPRA in the presence of 4 attackers. When increasing the number of attackers to 12, the detection accuracy of both the methods gets reduced. The PEPR avoids the attacker impersonation at the sender side using two-step authentication process, and also it exploits the random number with an original primitive polynomial function to confuse the attacker during overhearing. If any impersonation attackers act as an honest one, the CH easily identifies such attackers using check and verification polynomials. Also, if any intermediate node tries to serve as a destination for getting the data, the acknowledgments help to detect the attacker in the path. Then ExPRA detects only 25% attackers at the beginning due to the possibility for overhearing the key authentication. In the presence of 12 attackers, the ExPRA has 85% less detection accuracy than PEPR method. Since, when more than one intermediate routers have the same cluster ID, the attackers have the possibility to create the fake acknowledgment. In such cases, the detection accuracy is lesswhen increasing the number of attackers. However, the PEPR achieves relatively much better detection accuracy than ExPRA method.

8 Conclusion

This proposed paper has achieving secure and reliable data forwarding in highly dynamic networks using the detection and elimination of impersonation attackers. By enforcing these two separate transactions of the primitive

polynomial set with key function and the same with anyone random number in a Successive manner, the PEPR efficiently restricts the overhearing, as well as an attacker, does not hack the personal of a legitimate node. Thus, a severe impact of impersonation attacker has been reduced in clustered network. The novel clustering algorithm based network partition assist to elect the energy efficient and high worthy CH as well as reduce key overhead. By introducing the Energy efficient Polynomial Reduction (EPR) algorithm, the PEPR detects the attackers in the routing path with less overhead using consolidation method. Also, by exploiting the attackers in the routing path, accurately classifies and eliminates the attackers and announces such attackers to neighbor CHs for preventing the impersonation in the future. Finally, the simulation shows the better performance of PEPR than the existing ExPRA in terms, detection accuracy.

References

[1] K. V. Arya, S. S. Rajput, "Securing AODV routing protocol in MANET using NMAC with HBKS technique", in *IEEE International Conference on Signal Processing and Integrated Networks (SPIN'14)*, pp. 281–285, 2014.

[2] S. Balasubramani, S. K. Rani, S. Rajeswari, "Review on security attacks and mechanism in VANET and MANET", in *Artificial Intelligence and Evolutionary Computations in Engineering Systems*, pp. 655–666, 2016.

[3] M. Barbeau, J. Hall, and E. Kranakis, "Detecting impersonation attacks in future wireless and mobile networks", in *Secure Mobile Ad-hoc Networks and Sensors*, pp. 80–95, 2006.

[4] J. Ben-Othman and Y. I. S. Benitez, "A new method to secure RA-OLSR using IBE", in *Global Communications Conference (GLOBECOM'12)*, pp. 354–358, 2012.

[5] M. Chatterjee, S. K. Das, and D. Turgut, "WCA: A weighted clustering algorithm for mobile ad hoc networks", *Cluster Computing*, vol. 5, no. 2, pp. 193–204, 2002.

[6] J. Chen, J. Wu, "A survey on cryptography applied to secure mobile ad hoc networks and wireless sensor networks", in *Handbook of Research on Developments and Trends in Wireless Sensor Networks: From Principle to Practice*, pp. 262–289, 2010.

[7] J. H. Cho, R. Chen, "Model-based evaluation of distributed intrusion detection protocols for mobile group communication systems", *Wireless Personal Communications*, vol. 60, no. 4, pp. 725–750, 2011.

[8] N. Choudhary, L. Tharani, "A survey of routing attacks in mobile ad hoc network", in *IEEE Security in Wireless Mobile AD Hoc and Sensor Networks*, pp. 85–91, 2007.

[9] S. Djahel, F. Nait-Abdesselam, and Z. Zhang, "Mitigating packet dropping problem in mobile ad hoc networks: proposals and challenges", *IEEE Communications Surveys & Tutorials*, vol. 13, no. 4, pp. 658–672, 2011.

[10] A. Echchaachoui, A. Choukri, A. Habbani, and M. Elkoutbi, "Asymmetric and dynamic encryption for routing security in MANETs", in *IEEE International Conference on Multimedia Computing and Systems (ICMCS'14)*, pp. 825–830, 2014.

[11] P. D. Gawande, Y. Suryavanshi, "Cryptography based secured advanced on demand routing protocol in MANET's", in *IEEE International Conference on Communications and Signal Processing (ICCSP'15)*, pp. 1478–1481, 2015.

[12] D. Glynos, P. Kotzanikolaou, and C. Douligeris, "Preventing impersonation attacks in MANET with multi-factor authentication", in *IEEE Third International Symposium on Modeling and Optimization in Mobile, Ad Hoc, and Wireless Networks (WiOpt'05)*, pp. 59–64, 2005.

[13] T. Hayajneh, P. Krishnamurthy, D. Tipper, and T. Kim, "Detecting malicious packet dropping in the presence of collisions and channel errors in wireless ad hoc networks", in *IEEE International Conference on Communications*, pp. 1–6, 2009.

[14] R. H. Jhaveri, S. J. Patel, and D. C. Jinwala, "A novel approach for grayhole and blackhole attacks in mobile ad hoc networks", in *Second International Conference on Advanced Computing & Communication Technologies*, pp. 556–560, 2012.

[15] R. K. Kapur, S. K. Khatri, "Secure data transfer in MANET using symmetric and asymmetric cryptography", in *IEEE International Conference on Infocom Technologies and Optimization (ICRITO'15)*, pp. 1–5. 2015.

[16] P. Kavitha, R. Mukesh, "To detect malicious nodes in the mobile ad-hoc networks using soft computing technique", in *IEEE International Conference on Electronics and Communication Systems (ICECS'15)*, pp. 1564–1573, 2015.

[17] W. Kozma Jr, L. Lazos, "Dealing with liars: Misbehavior identification via Renyi-Ulam games", in *International Conference on Security and Privacy in Communication Systems*, pp. 207–227, 2009.

[18] M. K. Marina and S. R. Das, "Routing in mobile ad hoc networks", *Ad Hoc Networks*, pp. 63–90, 2005.

[19] M. M. Morshed, M. R. Islam, "CBSRP: Cluster based secure routing protocol", in *IEEE International Conference on Advance Computing (IACC'13)*, pp. 571–576, 2013.

[20] M. Sadeghi, S. Yahya, "Analysis of wormhole attack on MANETs using different MANET routing protocols", in *Fourth International Conference on Ubiquitous and Future Networks (ICUFN'12)*, pp. 301–305, 2012.

[21] T. Shu, M. Krunz, "Privacy-preserving and truthful detection of packet dropping attacks in wireless ad hoc networks", *IEEE Transactions on Mobile Computing*, vol. 14, no. 4, pp. 813–828, 2015.

[22] W. Wang, Y. Wang, "Secure group-based information sharing in mobile ad hoc networks", in *IEEE International Conference on Communications*, pp. 1695–1699, 2008.

[23] I. Woungang, S. K. Dhurandher, V. Koo, and I. Traore, "Comparison of two security protocols for preventing packet dropping and message tampering attacks on AODV-based mobile ad hoc networks", in *IEEE Globecom Workshops*, pp. 1037–1041, 2012.

[24] B. Wu, J. Chen, J. Wu, and M. Cardei, "A survey of attacks and countermeasures in mobile ad hoc networks", *Wireless Network Security*, pp. 103–135, 2007.

[25] Q. Wu, Y. Mu, W. Susilo, B. Qin, and J. Domingo-Ferrer, "Asymmetric group key agreement", in *International Conference on the Theory and Applications of Cryptographic Techniques*, pp. 153–170, 2009.

[26] W. Xu, W. Trappe, Y. Zhang, and T. Wood, "The feasibility of launching and detecting jamming attacks in wireless networks", in *ACM International Symposium on Mobile Ad Hoc Networking and Computing*, pp. 46–57, 2005.

[27] S. Zhang, Q. Cheng, and X. Wang, "Impersonation attack on two identity-based authenticated key exchange protocols", in *WASE International Conference on Information Engineering*, vol. 2, pp. 113–116, 2010.

Biography

P. Kavitha has acknowledged her B.E and M.E Degree in Computer Science and Engineering from National Engineering College in 2002 and 2004. She is presently pursuing her Ph.D in Hindustan Institute of Technology and Science, Chennai, Tamilnadu, India. She has nearly fourteen years of industrial, academic and research Experience. She is a member of IEEE. Her specialization area is Mobile Ad hoc Networks, Vehicular Ad hoc Networks, Cryptography and Network Security, Data mining and Software Engineering.

Dr. Rajeswari Mukesh has received her Ph.D. degree in Computer Science and Engineering from Jawaharlal Nehru University. Hyderabad. At present, she is a Professor and Head of School of Computing Sciences at Hindustan University, Chennai, Tamilnadu, India. She is guiding 8 PhD candidates. She has published above 10 international journals and attended beyond 15 international and National Conferences. Her area of specialization is Big Data, Biometrics, Adhoc Networks and Cyber Security. She is a Member of IEEE and IET. She has won the Women Engineer award recently from IET.