A Novel Integrated Scheme for Detection and Mitigation of Route Diversion Attack in MANET

H C Ramaprasad[1]
Research Scholar
Visvesvaraya Technological University
Belagavi, Karnataka, India

S.C. Lingareddy[2]
Professor and Head
Department of Computer Science and Engineering
SVCE, Bengaluru, Karnataka, India

***Abstract*—With the involvement of Mobile Adhoc Network (MANET) in many upcoming technologies and applications, there is an increasing concern about secure data transmission. Until the last decade, various solutions have evolved to circumvent this threat; however, the security issue is still a more significant threat. The problems studied during the review are usage of Complex Cryptographic Usage, Less Energy Efficient, Fewer studies towards Route Diversion Attack, and Less Emphasis towards Securing Beacon. An analytical method has been used to study these problems. This paper introduces a novel scheme that carries out dual operation viz. i) assessing the link legitimacy for detection of route diversion attack, and ii) cost-effective countermeasures for the same attack. The key findings of proposed study is token generation process when associated with link legitimacy offers more routing security from various ranges of threats. The broader implication of this finding is that proposed system when characterized by lightweight encryption operation, it is capable of excelling better balance between data transmission and security performance unlike existing security solutions in MANET.**

***Keywords*—Mobile Adhoc network; route diversion attack; routing attack; link legitimacy; encryption**

I. INTRODUCTION

Mobile Adhoc Network (MANET) offers a decentralized network of connected mobile nodes and can perform communication using any dependency towards infrastructure [1]. These mobile nodes are characterized by the formation of dynamic topology and have limited processing and storage capability. Secure routing among these mobile nodes is the better option to protect the communication in MANET. At present, there are various forms and taxonomies of secure routing protocol in MANET [2]-[4]. Each has its advantage as well as its limitations. The target of secure routing in MANET is to offer data protection from various potential threats in MANET in the complaint of security standards, i.e., non-repudiation, integrity, confidentiality, availability, authentication [5]. There are multiple types of reported attacks in MANET where the potential threats are classified into rushing attacks, fabrication attacks, impersonation attacks, and modification attacks [6]. Some of the potential attacks that target routing process in MANET are classified as i) common routing attacks -Cache poisoning attack over routing, Rushing attack, Packet replication attack, Overflow attack on routing table, and Poisoning attack on routing table, and ii) advanced attack-location disclosure attack, resource consumption attack, flooding attack, black hole attack, sleep deprivation attack [7]. Some of the conventional solutions to mitigate such attacks are Secure Efficient Ad-hoc Distance Vector, Ariadne, Secure Routing Protocol, Authenticated Routing for Ad-hoc Network, and Secure Ad-hoc On-Demand Distance Vector Routing [8]. Out of all this existing secure routing scheme, there is also much talk about the benefits of Optimized Link State Routing (OLSR) because of its beneficial communication features viz. i) confirms minimal delay in data transmission in MANET, ii) independent of any form of centralized scheme for managing data transmission and hence more suitable in MANET, iii) highly adaptable to dynamic changes in topology in MANET, and iv) freedom from link reliability for transmitting control message [9]. Owing to this reason, the adoption of OLSR is preferred compared to its other counterpart routing methodologies in MANET [10]. However, the adoption of OLSR in secure routing in MANET has seen very few research-based approaches in recent times. Some of the challenges that OLSR encounters when integrated with conventional encryption protocols are i) increased memory as it retains all information of routes and hence highly vulnerable for any routing attacks in MANET, ii) increased overhead with an increase of mobile host due to inclusion of encryption while it uses two different message, i.e., hello packet and topology control message, iii) not applicable for time-critical application as a considerable amount of time is required for an OLSR to identify faulty links, and iv) conventionally, OLSR demands more energy to perform route discovery process and hence when integrated with encryption, it consumes more power.

Therefore, this paper offers a solution meant to introduce a secured OLSR for resisting routing attacks considering the use case of route diversion attacks in MANET. It applies a lightweight encryption model, unlike any existing secure routing scheme. The model contributes towards a novel key management scheme without using any complex encryption scheme. The idea is to balance security demands without affecting the communication performance of mobile nodes. The paper organization is as follows: Section II discusses the existing literature followed by research problem in Section III. Methodology is discussed in Section IV, system design is discussed in Section V. Result is briefed in Section VI, while Section VII highlights outcome discussion, Section VIII makes conclusive remarks while Section IX briefs about future research direction.

II. Review of Literature

At present, various routing-based attacks are targeting to disrupt the communication system in MANET. It is also found that routing attack leads to incoming of multiple other forms of attacks in a decentralized environment in MANET. This section discusses all the practical approaches to mitigate such routing-based intrusion in MANET.

The recent work carried out by Cai et al. [11] have used a trust-based scheme to mitigate route disruption attacks in MANET. This scheme uses evolutionary techniques using the cognitive process of humans to resist such attacks in MANET, mainly meant for internal attackers. The existing system also emphasizes overusing authentication schemes for assessing the legitimacy of the link. The work of Tu et al. [12] has exploited the characteristic of active routing schemes towards resisting route spoofing, byzantine attack, false routing, selective forwarding attack, etc. The study outcome has witnessed a minimal increase in the packet delivery ratio. Jhaveri et al. [13] have used a pattern-based intrusion monitoring scheme over routing attacks leading to eavesdropping. The idea of this work is also to increase the security during the discovery of the routing phase. Route diversion attacks can also be in the shape of a wormhole attack in MANET. The recent work of Tahboush et al. [14] has presented a security scheme using the round trip time to reduce delay and explore the tunnel presented by wormhole attack. The study outcome is found to stop both in-band and out-band attacks by wormhole attackers by controlling the transmission range. The work of Li et al. [15] has presented a scheme capable of identifying the different variants of anomalies in MANET when exposed to a vulnerable routing scheme. The presented scheme presented an allocation and verification of the anomalies present in the dynamic environment of MANET.

The work carried out by Li et al. [16] has used reputation-based attributes to formulate the route. This technique has used a cooperative-based secure on-demand data transmission scheme to differentiate the selfish and malicious behavior of the node. The work carried out by Dhananjayan and Subbaiah [17] has used a trust-based technique to perform a better form of secure routing scheme in Adhoc networks. The uniqueness of this work is about the usage of the mobility model and energy attribute to understand an indicator for security. The work carried out by Mohindra and Gandhi [18] has presented a scheme where a clustering-based operation along with encryption is used for securing the data transmission in MANET. This technique has used a signature generation for a better authentication scheme. The presented method has used elliptical curve encryption to offer security and usage of digital signature. The work carried out by Mohammadani et al. [19] has used a unique access scheme to secure the data transmission in MANET. The unique part of this implementation is that the system uses time synchronization for all the time slots; however, it doesn't assign anything for blackhole attackers owing to the constant time slot.

Discussion about security strength of routing scheme in MANET based on the use of Internet-of-Things (IoT) is carried out by Trivedi and Khanpara [20]. Tripathy et al. [21] have developed an adaptive scheme for protecting the data transmission scheme in MANET from various attacks. The study presents a consideration of the context-based factors for specific factors to formulate trust values of the nodes. The existing system has also utilized fuzzy logic to address both security and quality of service in MANET. Rajashanthi and Valarmathi [22] carry out the work in such direction. In this study, an on-demand routing scheme along with fuzzy logic is used along with homomorphic encryption. The study has also used a bio-inspired algorithm to obtain a better route. The work carried out by Manjula and Anand [23] has implemented a key exchanged mechanism using Diffie-Hellman. The approach has used advanced encryption standards for encrypting data.

The existing system has presented different variants of approach where routing scheme along with various use-cases are considered for assessing security. The work carried out by Pu [24] has considered securing the communication from the flying Adhoc network to secure jamming and any other form of route disruption attack. It is also claimed by various researchers where reliability is potentially linked with securing communication in MANET. One such significant study has been presented by Liu et al. [25] that considers the cost of transmission and packet delivery ratio followed by evaluation of road weight. However, no significant evidence is found to offer resistivity against attackers. The work of Anand et al. [26] has presented a model capable of identifying the malicious behavior of MANET nodes. According to this scheme, a dynamic model of distributed form is developed along with the misbehavior of mobile nodes in the network to present preventing measures. The work of Smith et al. [27] has harnessed the potential of the existing security scheme capable of secure communication among mobile nodes, access control, and authentication of mobile nodes in MANET. The work carried out by Wang et al.[28] have developed a secure trust-based routing scheme where Petri net is used along with fuzzy logic to ascertain the eligibility of the nodes using OLSR protocol. Doss et al. [29] have presented a scheme for identifying and preventing novice forms of attack in MANET. This technique makes use of a learning approach for understanding the malicious behavior of mobile nodes. Usage of the learning scheme is also observed in Sankaran et al. [30], where the selection mechanism of the neighboring mobile node is secured in MANET. The learning scheme is used for reviewing the secure routing consistency. The following section discusses all the potential limitations explored after reviewing existing schemes of secure routing in MANET.

III. Research Problem

There are various mechanisms implemented to date to find out if the mobile node is a regular node and malicious node; however, there are few standard and effective research implementations towards exploring the legitimacy of the communication link. The initial implementation is more inclined to identify the precise legitimacy of link; however, the countermeasures offered are based on non-cryptographic mechanisms to ensure cost-effective modeling. Good resistivity cannot be ensured; however, delivering complex cryptographic measures is challenging to implement in WSN. The summarized version of the open end research problems found in existing studies are as follows:

- Complex Cryptographic Usage: There is no doubt that cryptographic algorithms offer the potential for resisting attacks in a wireless network. However, when it comes to MANET, the mobile nodes consistently drain energy along with its movement. It demands a novice cryptographic model that is lightweight and less iterative. The majority of the existing encryption mechanism uses extensive essential management operation, which requires the storage of secret keys, which are again vulnerable to various attacks in MANET.
- Less Energy Efficient: Existing secure routing schemes are more inclined towards data encryption and less on achieving optimal communication performance concerning data transmission. Majority of the existing techniques demands maximum resources to function in vulnerable scenario in MANET properly. Hence, there is a need for an encryption mechanism that is equally energy efficient when it comes to securing the data transmission scheme in MANET.
- Fewer studies towards Route Diversion Attack: Various approaches offer protection from routing-based attacks. But they are precisely not meant for route diversion attacks. To some extent, certain studies were carried out towards resisting wormhole attacks, which also bears nearly similar characteristics to route diversion attacks. However, the actual route diversion attack has received less attention as it is highly dynamic in its properties concerning the selection of the victim link. Moreover, the absence of any scheme for ascertaining link legitimacy is another reason for the lack of a standard solution towards route diversion attacks in MANET.
- Less Emphasis towards Securing Beacon: The complete route discovery process in MANET demands to broadcast its beacon. The attacker quickly captures such beacons, which can disclose various essential information related to application and network topology. Unfortunately, fewer OLSR based secure routers have addressed this problem in the last five years in MANET. The existing approaches don't emphasize protecting the beacons.

IV. Research Methodology

The proposed study continues our prior model SRDP [31], presenting a solution towards resisting route diversion attack. This work adds up furthermore lightweight security operations to offer more resilience. The implementation mechanism is highlighted in Fig. 1 as shown.

On top of SRDP architecture [31], the proposed system introduces a novel initialization stage where a sequential countermeasures process is carried out. The first stage of countermeasure is carried out by assessing the vulnerability in the link in MANET. In contrast, the second level of assessment is carried out considering multiple entity-based and entity-based single evaluations. The former type uses a mobile node and trusty third party while the latter uses only a mobile node to carry out an assessment. The proposed scheme uses homomorphic encryption to encrypt the data, followed by a series of encryption processes unlike any existing approach of resisting route diversion attacks. The experiment of this logic has been performed in MATLAB environment where the algorithms are written in the form of function, which will executed offers the results discussed in result section. The main target of the proposed system is to develop an analytical model that can identify route diversion attacks and mitigate them using a cost-effective optimal solution. The following section further elaborates on design and algorithm.

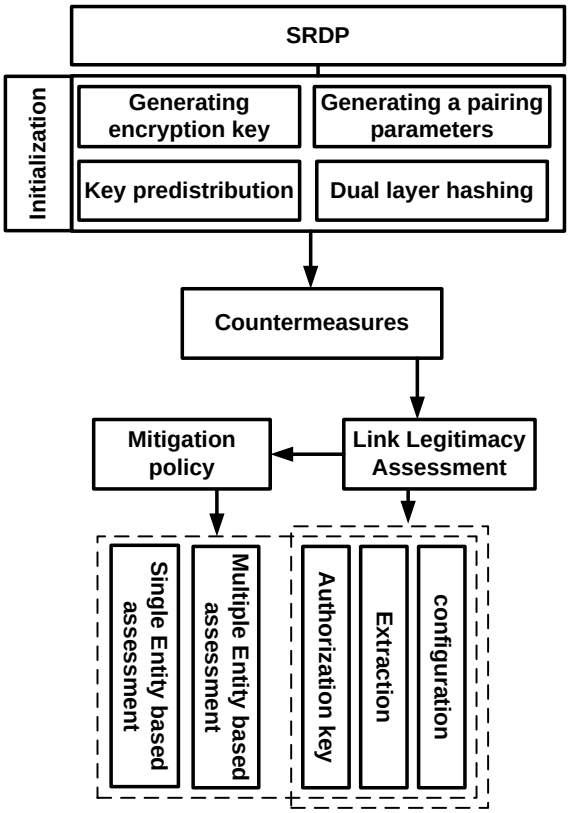

Fig. 1. Proposed Implementation Scheme.

V. System Design

This section discusses the essentials of the design aspects involved in the proposed implementation. The complete performance is classified into two stages where the first stage of implementation is wholly focused on generating the link legitimacy. In contrast, the second stage of implementation is focused on mitigating the intruder in the MANET environment. The elaborated discussion of both the implementation modules in the proposed system is as follows:

A. Algorithm for Link Legitimacy Token Generation

This algorithm is responsible for assessing the score of the vulnerability of the communication link among the mobile nodes in the dynamic environment of MANET. The idea is mainly to ensure that all the communicating links are secure enough to perform communication. The steps of the proposed algorithm are as follows:

Algorithm for Link Legitimacy Token Generation

Input: n_t (transmitting mobile nodes), Φ (core authority key)
Output: ψ (link legitimacy token)
Start
1. **For** i=1:n_t
2. S→n_t[Φ, π]
3. n_1(Φ)→λ_{ID}
4. n_1(B, ts, τ)→ψ
5. **For** ψ=valid
6. n_2(ID, B, ψ)→flag *accept*
7. **Else**
8. n_2(ID, B, ψ)→flag *reject*
9. **End**
End

This algorithm takes the input of transmitting mobile nodes n_t, core authority key Φ that after processing yields an outcome of link legitimacy token ψ. There are four sets of operations being carried out by this algorithm. The first set of actions of the algorithm is to carry out the configuration of essential actors present in the simulation study. Considering all the transmitting mobile nodes (Line-1), this algorithm lets a sink node generate a core attribute key Φ along with an attribute for private key generation π. All this information is then forwarded to the transmitting mobile node (Line-2). This completes the configuration step before the development of the communication model. The next set of actions for the proposed system is to perform an extraction of security information. In this process, the transmitting mobile node generates the authorization key τ associated with the identity ID using the core authority key Φ. This operation is related to the identity considered for the mobile transmitting mobile node (Line-3). After this operation, the proposed system feels a beacon B, timestamp ts, and an authorization key τ, the transmitting mobile node generates a link legitimacy token ψ (Line-4). The next operation step involves assessing the link legitimacy token by the receiving node n_2, which flags the outcome of acceptance of the validated link legitimacy token (Line-6) or invalid link (Line-8).

In this part of the proposed scheme, identity concatenated with time is considered a public key where the successive interval of times is obtained by the division of time. Further, homomorphic encryption is utilized to carry out the data where a dual hash function is used, viz. i) the first hash function is used for mapping the strings in the group while ii) the second hash function is used for mapping the random inputs. The first step in the process of link verification is extracting security information associated with it. The receiver node computes the private key.

$$\lambda_{receiver} = \text{hash}\ (ID_{receiver} \| t_s) \quad (1)$$

The expression (1) highlights the private key generated by the leader node LN. The next process is the mechanism of assessing the authorization key, which is generated as follows:

$$\tau_{receiver} = generator^{r} \quad (2)$$

In the above expression (2), the proposed system uses a generator considering r as a natural random number. Further, the system carries out concatenation of the broadcasted beacon along with its identity, timestamp, the security validation token of the receiver node over the ciphered data, and encrypted data. The computation of the security validation token *svt* of the receiver node over the ciphered data is carried out as follows:

$$svt = ct.\ \lambda_{receiver} + r_{receiver}.\text{generator} \quad (3)$$

In the above expression (3), the variable *ct* will represent ciphertext. The svt is incorporated within the data to ensure that no intruder could test the legitimacy of the link apart from the regular receiver node. The final step of this process is to assess the link legitimacy by the receiver node. For this purpose, the timestamp is evaluated concerning the current interval of time for the receiver node to find the freshness of the data received. After that, further computation is carried out by the receiver node:

$$\text{Generator}_{receiver} = A.\ e(B\text{-generator}_{public}) \quad (4)$$

In the above expression (4), the generator of the receiver is calculated concerning the following dependable parameters viz. i) *A*=(svt, generator), ii) B=hash($ID_{receiver}$||$ts_{receiver}$). If the condition is found to be validated concerning legitimate link, further expression (4) is progressively computed to yield an amended version of a conditional check as follow, which is if the value of *hash*($ct_{receiver}$||$ts_{receiver}$|| $\tau_{current}$)is equivalent to *hash*($ct_{receiver}$||$ts_{receiver}$|| τ_{old}), then the proposed system considers the link to be legitimate link and the message received from the link has higher data integrity. This message is further transmitted to another mobile node. Upon failure of this condition, all the communication with this link is aborted, and a new link is searched. From a security viewpoint, it can be seen that dependable parameters in all the mathematical expressions are entirely different. Hence, even if the message falls in intruder captivity, they will not find any link legitimacy information. Therefore, the algorithm offers a more straightforward link legitimacy assessment in MANET.

B. Algorithm for Countermeasure for Intruder

This algorithm continues the prior algorithm, which inherits its characteristics followed by mitigation strategy and targets towards mitigating the threat. The prior algorithm is about threat identification, while the second algorithm optimizes the first by incorporating mitigation measures. The steps of the proposed algorithm are as follows:

Algorithm for Countermeasure for Intruder

Input: n_t, Φ
Output: ψ_{me} / ψ_{se}
Start
1. **For** i=1:n_t
2. S→n_t[Φ, π]
3. LN(π, ts)→ ψ_{me}(n_{leaf})
4. n_{leaf} ($\lambda_{ID,}$ B)→ψ_{se}
5. **For** ψ=valid
6. n_2(ID, B, ψ_{se})→flag *accept*
7. **Else**
8. n_2(ID, B, ψ_{se})→flag *reject*
9. **End**
End

The algorithm mentioned above takes the input of transmitting mobile nodes n_t and core authority key Φ that, after processing, yields an outcome of link legitimacy token with multiple-single entity ψ_{me} / $\psi_{se.}$ This algorithm posses a similar configuration and extraction process as discussed in the prior algorithm for legitimacy check of link. The different operation carried out by this algorithm starts from Line-3. In this case, the algorithm performs two sets of novel operations, i.e., single entity assessment *se* and multiple entity assessment *me*. Numerous entities carry out the mechanism of the generation of the authorization key. In this case, the leader node LN generates link legitimacy token ψ_{me} using the attribute for private key generator π and time stamp *ts* (Line-3). This link legitimacy token is then forwarded to the mobile lead nodes in its group.

On the other hand, the algorithm also performs a single entity assessment where the transmitting leaf node n_{leaf} generates a link legitimacy token based on private key $\lambda_{ID(me)}$ and beacon B (Line-4). The final validation step is carried out from Line-5 onwards, where the mobile receiver node, i.e., $n_{2,}$ flags either acceptance or rejection based on the validated link legitimacy token. It should be noted that dependable parameters for this are carried out based on identity ID, beacon B, and link legitimacy token $\psi_{se.}$ This completes the operation of the proposed algorithm.

This algorithm mainly targets to reduce the possible overhead in the prior algorithm for identifying the degree of threat where the functionalities of distribution of security token are revised as follows: the prior algorithm assigns an attribute for private key generator with the highest number of parameters, i.e., encryption key, beacon, pairing parameters (elliptical curve, finite field), two discrete cyclic groups, bilinear map, global and local hash, generator, random integer. This algorithm uses a reduced number of parameters, i.e., encryption key, beacon, cyclic group, order of the cyclic group, random integer, random number of master key, and global hash. Similar homomorphic encryption is used in this part of the algorithm when the beacon B is transmitted to LN. In this algorithm, the receiver node obtains the private key from the core authority key Φ (randomly considered integer value) and node identity. The computation of the private key λ for receiver node uses two dependable attributes, e.g., k_1 and $k_{2,}$ where k_1 is equivalent to the randomly selected generator from the multiplicative group and k_2 is expressed mathematically as follows:

$$k_2=\text{rand}_{\text{receiver}} + hash(k_1, \text{ID}_{\text{receiver}}).\text{B} \quad (5)$$

In the above expression (5), the first component is a random number of mobile receiver nodes. In contrast, variable B of the second component represents a random natural integer (assuming it as core attribute key) and modulus of pairing parameter. The following process is for the usage of multiple entity-based assessments. A secure validation token *svt'* is generated by the receiver node along with the timestamp of transmission. This information is stored for carrying out a single entity-based assessment during beacon transmission. The mathematical expression of *svt'* is as follows:

$$\text{svt(me)} = 1 / \text{generator}^{ts} \quad (6)$$

The above expression is used for multiple entity assessment. The proposed algorithm also carry out a single entity assessment of vulnerability where a receiver node computes the link legitimacy token based on svt obtained in prior algorithm and randomly selected integer towards the encrypted data where svt' is created as follows:

$$\text{svt(se)}=\text{generator}^{\text{svt}} \quad (7)$$

The beacon is then forwarded by the mobile receiver node, the timestamp, randomly selected generator, and svt of a single entity. The beacon carries out the following information, i.e., the identity of the receiver node, timestamp, randomly selected generator. Finally, the algorithm proceeds towards the validation operation where all the mobile nodes perform validation of the received beacon. It starts with assessing the current time stamp, then computation of generator and product of svt randomly selected generator, and a random number. The proposed system also set a condition as follows:

$$\mu_1=svt.\ \mu_2.\ \mu_3 \quad (8)$$

In the above expression (8) for the conditional check, the variable μ_1 represents the mobile receiver node generator. In contrast, the variable μ_2 represents hashing of the random generator, and the variable μ_3 represents the random integer to the power of the hashed value of μ_2 and identity of the receiver node. A closer look at this algorithm's internal operation showcase that the proposed system introduces complex attributes for the attackers to perform intrusion. It is a complex process as the attacker will be required to decode multiple interconnected hashing operations with unknown variable definitions. The following section discusses the outcomes of the study.

VI. Result Analysis

This section discusses the outcomes obtained from implementing the algorithms discussed in the prior section. Scripted in MATLAB, the observations were carried out considering the following simulation parameters: i) several mobile nodes 1400, ii) initialized energy is 10J, iii) Size of the message is 1000 bytes, iv) total simulation rounds is 1000. The implementation environment involves the dispersion of mobile nodes in random order over a 1000x1000 m^2 simulation area. The mobile nodes form a group, and each group is assigned a leader node based on higher residual resources. The leader node carries out all the communication from one group to another, while a normal mobile node itself carries out communication within a group. The proposed system claims security in MANET considering the standard OLSR protocol; the comparison is carried out concerning the OLSR protocol. Irrespective of various availability of routing protocol, the justification behind selection OLSR are as following: i) the routing process of OLSR is decentralized and theoretically claimed to offer lower delay; however, still there is an issue with maintaining routing table for all sorts of routes, which is vulnerable for attack in MANET, ii) it offers supportability of dynamic changes in MANET; however, it also witnesses higher beacon overhead and consumes more processing power. Moreover, the proposed study is implemented in order to address such issues in OLSR. To closely observe the outcome,

the proposed method is split into Prop-1 and Prop-2, exhibiting the algorithm for link legitimacy and cost-effective countermeasures. The outcome analysis concerning standard performance parameters in MANET is mainly associated with resource utilizing, delay, and packet delivery ratio.

The first performance parameter used towards investigating the effect on communication performance is resource depleted nodes. After initializing the nodes with energy, there is a decrement in power. The idea of these performance parameters is to check the availability of nodes in the proposed security scheme.

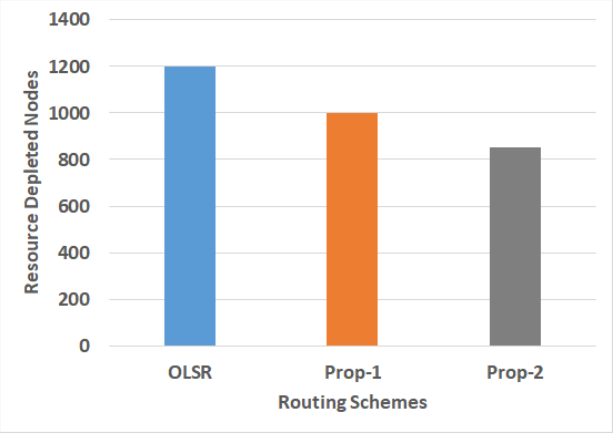

Fig. 2. Comparative Analysis of Resource Depleted Nodes.

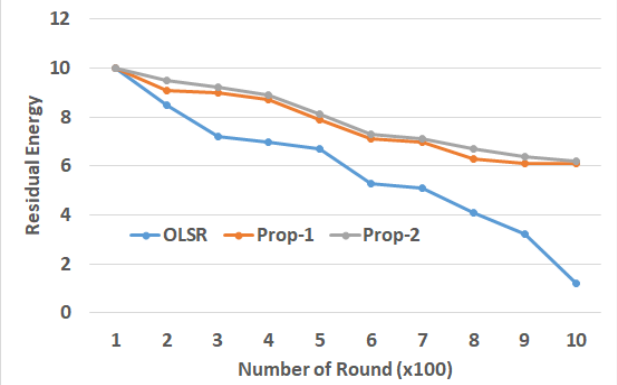

Fig. 3. Comparative Analysis of Residual Energy.

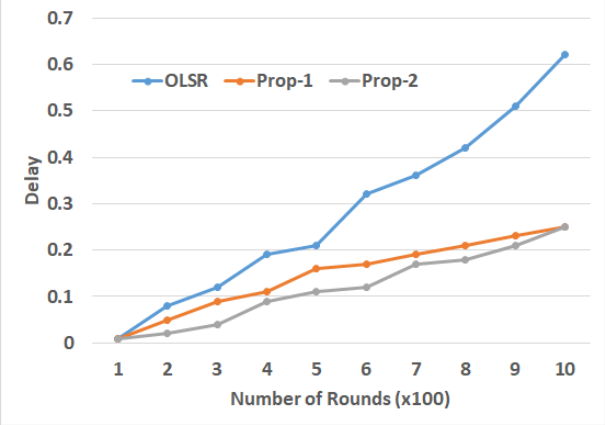

Fig. 4. Comparative Analysis of Delay.

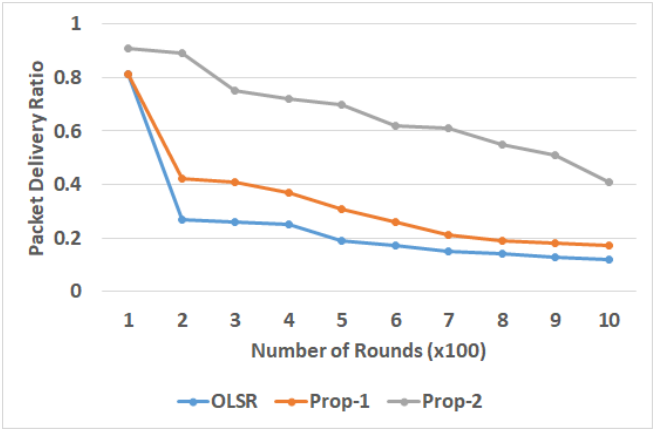

Fig. 5. Comparative Analysis of Packet Delivery Ratio.

Fig. 2 to Fig. 5 represents comparative analysis of the proposed system (with two variants) with the existing standard OLSR protocol with respect to resource being depleted, residual energy, delay, and packet delivery ratio respectively. In every case, the proposed system is witnessed to offer superior outcome in contrast to OLSR protocol.

VII. Discussion

This section discusses about the outcome obtained from the proposed study briefed in prior section.

- Discussion of Resource Depleted Nodes (Fig. 2): The outcome exhibited in Fig. 2 showcases that the proposed system offers better node availability than the existing system. OLSR scheme is much occupied into formulating topology control which increases its resource dependency when the encryption scheme is applied along with OLSR. On the contrary, the Prop-1 scheme also does a similar job finding link vulnerability owing to route diversion attacks. However, this scheme uses more random numbers and generators and more minor encryption operations, leading to lesser resource consumption than OLSR. On the other hand, the extensive usage of parameters in key distribution is further controlled in Prop-2, leading to further saving of resources in contrast to Prop-1. The following associated performance study is towards residual study to validate the prior outcome of node availability.
- Discussion of Residual Energy (Fig. 3): As exhibited in Fig. 3, it can be seen that the depletion of energy for Prop-2 and Prop-1 is far better than the OLSR protocol. This ensures that with the increase of simulation rounds (where traffic load is also increased), the proposed scheme can successfully achieve better retention of energy and better node availability. The following performance parameter understudy is an end-to-end delay, a duration involved in packet transmission from transmitting to receiving mobile nodes in MANET. The outcome of the delay is shown in Fig. 4.

- Discussion of Delay (Fig. 4): The outcome in Fig. 4 exhibits that OLSR offers extensive delay compared to the proposed scheme. The prime reason is the involvement of multi-point relay and extensive cryptographic mechanism; the establishment of the route takes time in the presence of traffic load with increasing simulation rounds. Apart from this, the involvement of time for multi-point relay further adds to more delay. However, an operation carried out in Prop-1 involves conditional checks more and less encryption, which involves less duration. Further, Prop-2 offers the advantage of updating the link legitimacy token with a recent time stamp, which further authenticates the link with the presence of a route diversion attack. This causes lesser dependency on performing repeated route discovery processes in Prop-2. Apart from this, the inclusion of group-based communication also contributes towards lower delay. Finally, the proposed system assesses data forwarding performance via packet delivery ratio computed by cumulative data received at the destination and forwarded by transmitting mobile nodes.
- Discussion of Packet Delivery Ratio (Fig. 5): Fig. 5 showcases that the proposed system offers a better packet delivery ratio in comparison to OLSR. With the depletion of energy, the trend of packet delivery ratio will also degrade. The prime reason behind this outcome is that once the mobile node deletes its energy in OLSR, the number of relay nodes is significantly affected in formulating better routes. A further change of topology also involves time, and hence increasing the number of data when subjected to encryption further takes a slow performance in OLSR. However, this problem is mitigated in the proposed system by group-based communication using a leader node with forwarding aggregated data from its candidate mobile node in the proposed scheme. The difference between OLSR and Prop-1 is that – in OLSR, a single mobile node performs complete data transactions. In contrast, the proposed scheme performs aggregated data transmission via leader node, which saves time and increases the data transmission rate. However, Prop-1 has extensive usage of key management mechanism which is optimized in Prop-2 model and hence, the Prop-2 model offers further better outcomes than the Prop-1 model.
- Discussion of Security Analysis: It is to be noted that although the proposed system is designed towards resisting route diversion attacks, it still offers intrusion prevention capabilities furthermore. Owing to the usage of homomorphic encryption, the proposed method (Both Prop-1 and Prop-2) offers resistance from eavesdropping. Due to a series of dependencies towards the verification process, the proposed system doesn't allow the intruder to decrypt the ciphered beacon and data, ensuring optimal privacy and confidentiality. Apart from this, the encryption process considers identity, which will offer privacy protection for the mobile nodes in MANET. Another interesting fact is that the proposed system communicates via the leader node, which possesses extensive information to be forwarded or received. Hence, they are more prone to attack. It should be noted that Prop-2 is mainly carried out towards protecting the leader node, while Prop-1 is carried out towards protecting the mobile node. Hence, there is no feasibility of an active attack as well.

VIII. Conclusion

Route diversion attack is a severe problem in the dynamic environment of MANET. Irrespective of various research works towards resisting such routing attacks; the existing scheme lacks autonomous precise monitoring and a robust prevention scheme. Hence, the proposed system offers a solution against this problem by introducing an integrated computational model that offers a scheme to confirm link legitimacy and prevent attackers in MANET. The contribution and novelty of the proposed study are as follows: i) The proposed scheme offers an asymmetric essential management technique potential enough to stop eavesdropping along with resisting routing attacks, ii) The proposed model facilitates neighborhood authentication unlike conventional secure OLSR model in MANET, iii) the proposed model uses lightweight encryption mechanism to over low storage cost and comparatively higher network scalability, and iv) the proposed model offers a good balance between optimal security performance with efficient data transmission performance in MANET.

IX. Future Work

After reviewing the outcomes and their inference, it has been noticed that with a unique proposed research methodology without using complex form of cryptography. However, there are few questions which is further required to be analyzed viz. i) can be memory used for processing secret key be optimized? ii) can any non-encryption based operation be performed on top of this model in order to offer more privacy and further more security? Working toward these questions will be a part of future plan of implementation. The future work of the proposed study is to carry out implementation of bio-inspired algorithm to address the question of memory optimization for secret key processing. Further, trust based stochastic modelling can be carried out in order to address the second question towards deploying non-encryption based approach for offering more privacy and security. Deep learning method can be also further applied in order to generate attack graph in preemptive form prior the actual attack takes place.

References

[1] M. Al Mojamed, "Integrating Mobile Ad Hoc Networks with the Internet Based on OLSR", *Hindawi-Wireless Communications and Mobile Computing*, Article ID 8810761, 2020.

[2] Kalime, Srinivas & Sagar, K. “A Review: Secure Routing Protocols For Mobile Adhoc Networks (MANETs)”, *Journal of Critical Reviews*, vol.7, pp.8385-8393, 2021.

[3] H. Yang, "A Study on Improving Secure Routing Performance Using Trust Model in MANET", *Hindawi-Mobile Information Systems*, Article ID 8819587, 2020.

[4] G. M. Borkar; A.R. Mahajan, "A review on propagation of secure data, prevention of attacks and routing in mobile ad-hoc networks", *InderScience-International Journal of Communication Networks and Distributed Systems*, vol.24, No.1, 2020.

[5] M. S. Sheikh, J. Liang, "Security and Privacy in Vehicular Ad Hoc Network and Vehicle Cloud Computing: A Survey", *Hindawi-Wireless Communications and Mobile Computing*, Article ID 5129620, 2020.

[6] M. Karthigha, L. Latha and K. Sripriyan, "A Comprehensive Survey of Routing Attacks in Wireless Mobile Ad hoc Networks," *International Conference on Inventive Computation Technologies*, pp. 396-402, doi: 10.1109/ICICT48043.2020.9112588, 2020.

[7] R. Meddeb, B. Triki, F. Jemili and O. Korbaa, "A survey of attacks in mobile ad hoc networks," *International Conference on Engineering & MIS* (ICEMIS), 2017, pp. 1-7, doi: 10.1109/ICEMIS.2017.8273007.

[8] C. Ran, S. Yan, L. Huang & L. Zhang, "An improved AODV routing security algorithm based on blockchain technology in ad hoc network" *EURASIP Journal on Wireless Communications and Networking*, 2021.

[9] T. K. Priyambodo, D. Wijayanto, and M. S. Gitakarma, "Performance Optimization of MANET Networks through Routing Protocol Analysis", *MDPI-Journal*, vol.10, No.2, 2021.

[10] Y. Maret, J. -F. Wagen, M. Raza, J. Wang, N. Bessis and F. Legendre, "Preliminary results of OLSR based MANET routing algorithms: OLSRd2-Qx reinforcement learning agents and ODRb," *International Conference on Military Communication and Information Systems* (ICMCIS), 2021, pp. 1-8, doi: 10.1109/ICMCIS52405.2021.9486409.

[11] R. J. Cai, X. J. Li and P. H. J. Chong, "An Evolutionary Self-Cooperative Trust Scheme Against Routing Disruptions in MANETs," *IEEE Transactions on Mobile Computing*, vol. 18, no. 1, pp. 42-55, 1 Jan. 2019, doi: 10.1109/TMC.2018.2828814.

[12] J. Tu, D. Tian and Y. Wang, "An Active-Routing Authentication Scheme in MANET," *IEEE Access*, vol. 9, pp. 34276-34286, 2021, doi: 10.1109/ACCESS.2021.3054891.

[13] R. H. Jhaveri, N. M. Patel, Y. Zhong and A. K. Sangaiah, "Sensitivity Analysis of an Attack-Pattern Discovery Based Trusted Routing Scheme for Mobile Ad-Hoc Networks in Industrial IoT," *IEEE Access*, vol. 6, pp. 20085-20103, 2018, doi: 10.1109/ACCESS.2018.2822945.

[14] M. Tahboush and M. Agoyi, "A Hybrid Wormhole Attack Detection in Mobile Ad-Hoc Network (MANET)," *IEEE Access*, vol. 9, pp. 11872-11883, 2021, doi: 10.1109/ACCESS.2021.3051491.

[15] T. Li, J. Ma, Q. Pei, H. Song, Y. Shen and C. Sun, "DAPV: Diagnosing Anomalies in MANETs Routing With Provenance and Verification," *IEEE Access*, vol. 7, pp. 35302-35316, 2019, doi: 10.1109/ACCESS.2019.2903150.

[16] Z. Li and H. Shen, "Game-Theoretic Analysis of Cooperation Incentive Strategies in Mobile Ad Hoc Networks," *IEEE Transactions on Mobile Computing*, vol. 11, no. 8, pp. 1287-1303, Aug. 2012, doi: 10.1109/TMC.2011.151.

[17] G. Dhananjayan & J. Subbiah, "T2AR: trust-aware ad-hoc routing protocol for MANET", *SpringerOpen*, Vol.5, Article No. 995, 2016.

[18] A. R. Mohindra, C. Gandhi, "A Secure Cryptography Based Clustering Mechanism for Improving the Data Transmission in MANET", *Walailak Journal of Science and Technology*, Vol.18, No.6, 15 March 2021.

[19] K. H. Mohammadani, K. A. Memon, I. Memon, I. Memom, "Preamble time-division multiple access fixed slot assignment protocol for secure mobile ad hoc networks", *International Journal of Distributed Sensor Networks*, 2020.

[20] R. Trivedi, P. Khanpar, "Robust and Secure Routing Protocols for MANET-Based Internet of Things Systems—A Survey", *Springer-Emergence of Cyber Physical System and IoT in Smart Automation and Robotics*, pp 175-188, 2021.

[21] B. K. Tripathy, S. K. Jena, P. Bera & S. Das , "An Adaptive Secure and Efficient Routing Protocol for Mobile Ad Hoc Networks", *Springer-Wireless Personal Communication*, vol.114, pp.1339-1370, 2020.

[22] M. Rajashanthi & K. Valarmathi, " A Secure Trusted Multipath Routing and Optimal Fuzzy Logic for Enhancing QoS in MANETs", *Springer-Wireless Personal Communications*, vol.112, pp.75–90, 2020.

[23] T. Manjula & B. Anand, "A secured multiplicative Diffie Hellman key exchange routing approach for mobile ad hoc network", *Springer-Journal of Ambient Intelligence and Humanized Computing*, vol.12, pp.3621–3631, 2021.

[24] C. Pu, "Jamming-Resilient Multipath Routing Protocol for Flying Ad Hoc Networks," IEEE Access, vol. 6, pp. 68472-68486, 2018, doi: 10.1109/ACCESS.2018.2879758.

[25] L. Liu, C. Chen, B. Wang, Y. Zhou and Q. Pei, "An Efficient and Reliable QoF Routing for Urban VANETs With Backbone Nodes," *IEEE Access*, vol. 7, pp. 38273-38286, 2019, doi: 10.1109/ACCESS.2019.2905869.

[26] A. Anand, H. Aggarwal and R. Rani, "Partially distributed dynamic model for secure and reliable routing in mobile ad hoc networks," *Journal of Communications and Networks*, vol. 18, no. 6, pp. 938-947, Dec. 2016, doi: 10.1109/JCN.2016.000128.

[27] D. Hurley-Smith, J. Wetherall and A. Adekunle, "SUPERMAN: Security Using Pre-Existing Routing for Mobile Ad hoc Networks," *IEEE Transactions on Mobile Computing*, vol. 16, no. 10, pp. 2927-2940, 1 Oct. 2017, doi: 10.1109/TMC.2017.2649527.

[28] X. Wang, P. Zhang, Y. Du and M. Qi, "Trust Routing Protocol Based on Cloud-Based Fuzzy Petri Net and Trust Entropy for Mobile Ad hoc Network," *IEEE Access*, vol. 8, pp. 47675-47693, 2020, doi: 10.1109/ACCESS.2020.2978143.

[29] S. Doss et al., "APD-JFAD: Accurate Prevention and Detection of Jelly Fish Attack in MANET," *IEEE Access*, vol. 6, pp. 56954-56965, 2018, doi: 10.1109/ACCESS.2018.2868544.

[30] K. S. Sankaran, N. Vasudevan, K. R. Devabalaji, T. S. Babu, H. H. Alhelou and T. Yuvaraj, "A Recurrent Reward Based Learning Technique for Secure Neighbor Selection in Mobile AD-HOC Networks," *IEEE Access*, vol. 9, pp. 21735-21745, 2021, doi: 10.1109/ACCESS.2021.3055422.

[31] Ramaprasad, H & Lingareddy, S., "SRDP: Secure Route Diversion Policy for Resisting Illegitimate Request in MANET", *International Journal of Engineering & Technology*, vol.7. No.290. 10.14419/ijet.v7i3.12.16044, 2018.