Securing Dynamic Source Routing by Neighborhood Monitoring in Wireless Adhoc Network

Rajani K C[1]
Assistant Professor
Department of Computer Science and Engineering, Sea College of Engineering and Technology, Bangalore, India

Aishwarya P[2]
Professor and HoD
Department of Computer Science and Engineering
Atria Institute of Technology, Bangalore, India

***Abstract*—Wireless Adhoc Network (WANET) significantly contributes to cost-effective network formulation due to decentralized and infrastructure-less schemes. One of the primary forms of WANET in Mobile Adhoc Network (MANET) is still evolving in research and a continued set of research problems associated with security. A review of existing security approaches shows that identifying malicious behavior in MANET is still an open-end problem irrespective of various methods. This paper introduces an improved DSR protocol mechanism of neighborhood monitoring scheme towards analyzing the malicious behavior in the presence of an unknown attacker of dynamic type. The proposed method contributes to deploying auxiliary relay nodes and retaliation nodes to control the communication process and prevent the attacker from joining the network. Using analytical research methodology, the proposed system can offer better communication performance with effective resistance from threats in MANET.**

Keywords*—Mobile adhoc network; wireless adhoc network; security; attack; dynamic source routing

I. Introduction

The current research work is focused on deploying a security feature for identifying the threat followed by preventing the threat in Wireless Adhoc Network (WANET). Used in multiple forms of wireless application, adoption of WANET offers better connection as well as it also invite various levels of threats. Basically, a WANET is a decentralized scheme used in the wireless network with zero dependencies towards any infrastructure [1]. Theoretically, it is further classified into Wireless Sensor Network (WSN), Mobile Adhoc Network (MANET), and Wireless Mesh Network (WMN). However, from a practical viewpoint, the mapping of WANET is more carried out towards the MANET environment characterized by various constraints, e.g., low resource availability, lower processing capability, decentralized, and dynamic topology [2]. Besides, establishing a potential route among mobile nodes in a dynamic environment irrespective of various routing-based research approaches [3]. Owing to this limitation in MANET, there is a likely probability for any mobile node to reject forwarding data packets and thereby act as a malicious node. At present, there are various forms of security threats in MANET, and ongoing research is attempting to solve this problem to a maximum extent using different approaches [4][5]. Out of all the security threats, the most challenging task is to confirm the identification of the malicious node. The route discovery process is usually targeted during malicious routing intrusion, which leads to consequences where the mobile nodes don't comply with the assigned routing protocol [6]. Hence, it is essential to incorporate an effective routing scheme. Any mobile node that doesn't cooperate in data packet forwarding can be termed malicious and selfish nodes. However, there are more possibilities for defining the roles of such nodes. A regular node and malicious nodes are easier to identify; the challenge is only towards identifying any node with vulnerable behavior regarding routing. There is no statutory value to determine this scale of vulnerability to be confirmed as attacker node, compromised node, or selfish node. Various studies are being carried out to identify the malicious behavior in MANET [7]-[9]. However, there is still limitation associated with it, viz. i) excessive usage of encryption or complex secure routing techniques leads to loss of balance between communication and security, ii) adherence to a specific form of the attacker, iii) less emphasis towards dynamic attacking strategy. If this problem is not solved that the secondary issues owing to the presence of malicious nodes cannot be solved, viz. i) degradation in network connectivity, ii) isolated nodes with prominent declination in network performance, iii) less conservation of resources, iv) leads to exposure towards other forms of attackers. Hence, it is necessary to develop a security solution considering dynamic attackers without predefined information. In this perspective, the proposed system considers using Dynamic Source Routing (DSR) protocol owing to its beneficial features of being a reactive protocol in MANET [10].

However, there is less number of studies being investigated towards harnessing the potential of DSR protocol as the baseline of secure routing. It is also associated with a limitation which doesn't facilitate the mobile nodes to carry out operations towards identifying malicious behavior of mobile nodes. The proposed system uses DSR and improves its functionalities towards incorporating neighborhood monitoring states of the mobile nodes. The novelty is to detect and prevent unknown attackers of dynamic form present in MANET, whereas existing approaches mainly deal with the static form of attackers. Another novelty is about retaliation node to perform outlier management to present a unique mitigation measure. The paper's organization is as follows: Section II discusses existing approaches, while its limitation in the form of the research problem is addressed in Section III. The proposed methodology is discussed in Section IV. System

design is elaborated in Section V. Section VI discusses the outcomes obtained, while discussion of learning outcomes is presented in Section VII. The conclusion is given in Section VIII.

II. Existing Techniques

This section discusses the existing approaches towards securing Wireless Adhoc Network (WANET) towards identifying and mitigating malicious behavior of nodes. Current methods have witnessed the usage of trust-based mechanisms for mitigating malicious behavior. The work carried out by Abbasi et al. [11] has developed a scheme to secure message exchange operation towards vehicular Adhoc networks using a clustering algorithm concerning vehicle reputation. Irrespective of sound validation of the model, this approach doesn't resist the threat if the attacker is unknown. Another trust-based method was formulated by Chen et al. [12], considering a case study of internet-of-vehicles. The study has presented a collaborative scheme for filtering the behavior of regular to malicious nodes based on small-time intervals. The system also facilitates indirect trust calculation based on obtained recommendations from the adjacent nodes. The study is limited to resisting collusion attacks. Hence, the reputation factor also plays a significant role in identifying the malicious nature of nodes in WANET. A study towards emphasizing reputation is carried out by Guaya-Delgado et al. [13], where a unique routing scheme is constructed based on source routing. The core idea of this study is to identify any form of abnormal changes in the behavior of nodes considering routing behavior to be stationary. The study's outcome is limited for its effectiveness only concerning resisting selfish nodes in MANET.

Further study towards trust-based communication is presented by Dhananjayan and Subbaiah [14], where the conventional AODV protocol is rendered more secure considering all the essential constraints in MANET. The prime notion of this study is to match the ID of the packet sequence obtained from log traces of adjacent mobile nodes to assess the rate of trust. The target is to resist the generation of any form of a report by the malicious node. The study inherits the limitation as stale routing issues in AODV are not addressed. Janani and Manikandan [15] have presented a trust management scheme using Evidence Theory and Bayesian Theoryto validate malicious behavior detection. The study has emphasized understanding the degree of uncertainty in determining malicious behavior. However, the study offers a highly iterative scheme to identify malicious behavior inapplicable towards dynamic attackers in the MANET environment. A study toward evidence theory is further carried out by Mowla et al. [16]. The idea was to develop a cognitive learning scheme for the detection and mitigation of the jamming attack. The assessment of the study is carried out using a standard attack dataset for jamming intrusion. The applicability of the study is limited to jamming attacks only.

Further improvement in trust-based schemes towards malicious behavior detection is reported in Khan et al. [17], where multi-trust attributes are considered over-optimized link-state routing. The study is meant to resist multiple security threats; however, the formal model verification doesn't consider the dynamic alteration of attack strategy in MANET. The study of Kavitha et al. [18] has presented a security technique using optimized features followed by a classification scheme in MANET. The idea is to safeguard the Adhoc network from isolation attacks where neural network and particle swarm optimization have been used to optimize the features. Similar machine learning is used for classifying the attacker node. One of the potential pitfalls of this study is its dependency on training operations, which may bypass sure attackers using different strategies. Faisal et al. [19] have carried out a study to resist replication attacks, Sybil attacks, and impersonation attacks based on their received signal strength. This is done to find out the usage of additional hardware by the attacker. The security effectiveness of this study is limited to only the attacks mentioned above.

At present, blockchain was also reported to be used for resisting threats in MANET concerning its malicious behavior, as reported in the work of Ran et al. [20]. The researcher has used the AODV protocol, where blockchain is used for network development considering constraints. Although this is quite a novel approach with more applicability on future network technologies, the deployment of blockchain constructed is higher centralized, affecting the scalable performance in MANET. A unique study is carried out by Yasin and Zant [21], where the authors have presented a bait technique using a timer to identify and isolate attacks; however, the study applicability is limited to resist blackhole attacks only. Wireless Sensor Network is also a form of WANET system where existing approaches have been witnessed to mitigate identification issues of threats. The work of Alghamdi et al. [22] has used a convolution technique that generates security bits to resist attacks from malicious nodes using convolution codes. The simulated outcome shows the proposed scheme to offer better overhead control with better data transmission performance. However, the model doesn't provide prevention from any form of internal attacker. Wang et al. [23] have carried out a study where the bio-inspired protocol is designed for trust evaluation. The study offers the benefits of optimization, but it is not meant for resisting dynamic attackers.

Recent studies are being carried out where Dynamic Source Routing (DSR) is seen as the better option for securing threats in MANET. There is the evolution of various security-based schemes on DSR protocol viz. Bio-inspired algorithm (Almazok and Bilgehan [24]), cognitive-based DSR (Begum et al. [25]), trust-based scheme (Ishmanov and Zikria [26]), distributed key-generation (Kojima et al. [27]), path reliability-based approach (Liang et al. [28]), resisting blackhole attack (Mohanpriya et al. [29]), digital signature-based acknowledgment scheme (Srivastava et al.[30]).

From the above discussion of existing studies, it can be seen that there are good availability of research work towards securing wireless adhoc network. The methods mentioned above use different mitigation measures considering a specific case study in an Adhoc environment. Irrespective of reported benefits, there are various pitfalls towards the mechanism for securing adhoc network. Apart from this, it is also seen that existing approaches are deployed towards singular form of adversary whereas it is really a challenging one to identify if

the attacker alters its behaviour in WANET environment. Therefore, there is a need of a study which can address such issues. However, these schemes are more addressed towards specifics of adversary environment in deployment scene. The following section presents possibilities of various pitfalls associated with existing security approaches.

III. Research Problem

After reviewing the existing security approaches from the prior section, the following conclusive remarks has been drawn associated with the limitation of the methods:

- Scattered Approaches for Malicious Behaviour: There are split approaches towards different variants of the Adhoc network. However, there is no generalized scheme that is meant for all the variants of the Adhoc network. Due to varying operations in sensor networks and mobile Adhoc networks, a particular method cannot be used to secure both. Eventually, malicious behavior of a single form of attack will implicate different forms of consequences in other variants of the Adhoc network. There is less availability of standard generalized scheme towards, which impose as an impediment towards security incorporation.
- Unproportionate Schemes of Implementation: It has been seen that trust-based schemes are frequently used to resist attacks. However, trust-based schemes are developed based on direct and indirect trust computation without considering the dynamicity involved in the topology in a mobility environment. Apart from this, not much emphasis is offered to support a decentralized environment in a mobility environment. Other schemes are also available, e.g., evidence theory, machine learning, encryption, etc. However, their systems are still evolving, and no significant benchmarking is carried out to prove their applicability and effectiveness.
- Biased adversary model: Most studies have predefined information of the adversary, where it is not a challenging task to stop such an attack. However, these schemes are not applicable if the adversary changes its attack strategies. None of the existing studies are reported to work on dynamic attackers, which render the non-applicability of such algorithms in large-scale environments.
- More emphasis on prevention: A better form of prevention requires a better aggregation of the adversary's attack strategies. However, as the existing approaches have apriori information about the attackers, such prevention is only ensured for considered attacks and not for unknown attackers.
- More miniature Simplified Modelling: In the case of MANET, the mobile nodes consistently drain their energy and other resources. Hence, a robust security approach that requires consistent neighborhood monitoring will drain more energy for such resource-constrained mobile nodes. This demands much lightweight security operation, whereas the existing scheme offers more complex forms of the process that are less practical in the real world.

Hence, based on the research mentioned above problem, the statement is "identification of malicious behavior for the unknown attacker in decentralized mobility environment in Adhoc network is challenging task". The following section outlines the adopted research methodology which is meant for addressing the above mentioned research problems.

IV. Research Methodology

The implementation of the proposed system is carried out as an extension of our prior model of retaliation to identify the selfish node. This part of the implementation contributes to i) developing a novel secure DSR protocol and ii) the unique identification and prevention strategy towards malicious behavior of an unknown attacker in the MANET environment. The implemented architecture of the proposed system is as follow:

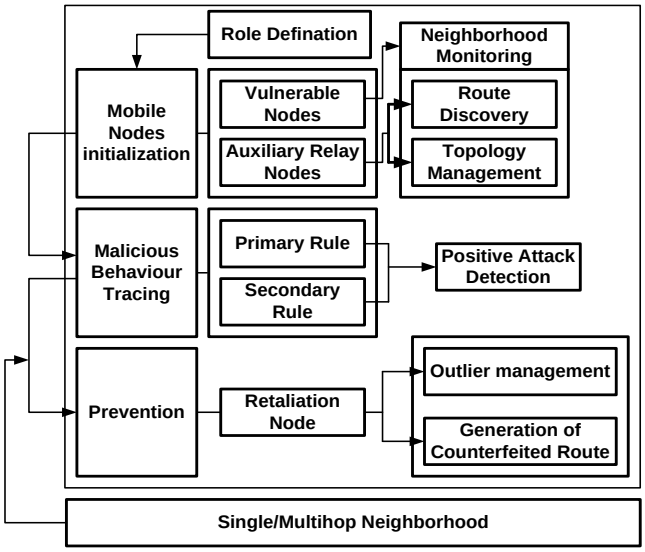

Fig. 1. Proposed Architecture of Secured DSR

Fig. 1 highlights the top-down architecture of the proposed secured DSR protocol in MANET. There are three significant operation blocks, i.e., i) mobile node initialization, ii) malicious behavior tracing, and iii) prevention. The first block of operation incorporates novel roles in mobile nodes by introducing vulnerable nodes and auxiliary nodes, unlike any existing approach of using DSR in MANET. The second block of process traces malicious behavior where two significant rules are developed to confirm the vulnerability as positive attack nodes. This rule formation assists in performing scrutiny of control messages of all nodes to ascertain their legitimacy using a novel algorithm for detecting a threat. Once the threat is positively detected, the last block of operation prevents the attackers by introducing a retaliation node. The novelty of the proposed system is the mechanism of resisting threats by retaliation node revised from our previous study. This node doesn't have its physical presence, and it is advertised by the target node under security observation when witnessed with the positive threat. The prime responsibility of this node is first to assess the update information of single and multihop

neighborhood nodes of vulnerable nodes. It generates counterfeited routes that don't match with any of the routes maintained in hop tables. To perform accurate detection, a probability-based computation is carried out to find out outliers in the detection process. The novelty of this approach is that it deploys a mechanism without using conventional encryption to secure the complete network system. It also introduces a special form of retaliation node which carries out this process of security incorporation. The following section discusses the system design.

V. System Design

This section discusses the proposed scheme implementation targeted towards mitigating routing misbehavior in DSR protocol in MANET. This section discusses the strategies used for designing the scheme and algorithm implementation.

A. Strategies Towards DSR Implementation

DSR is an on-demand routing scheme that utilizes a source-routing scheme that specifies the data sender's routes (complete or partial). The address of all the mobile nodes is required to determine the source route while performing route discovery in MANET. Caching is carried out for the aggregated information of path by the mobile nodes, which are used for the forwarding data packet. As the routed data consists of participating mobile nodes; hence, there are chances of intrusion and high overhead for large-scale network topology. Although conventional DSR protocols offer hop-by-hop communication for packet transmission to resist this overhead issue, identifying the unknown threat and disclosing the information is the biggest challenge. The mechanism of DSR is shown in Fig. 2 that carries out the a) route discovery and b) updating process in the MANET environment.

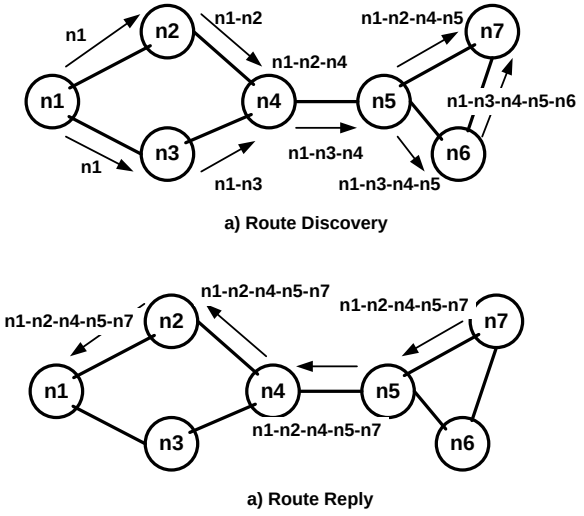

Fig. 2. Mechanism of Conventional DSR Scheme.

Implementing DSR protocol requires formulating two routing stages: i) discovery of routes and ii) route maintenance. The generation of route response beacon in DSR is carried out only when the destination mobile node has successfully. The destination node should possess the route information towards the original mobile node to forward the response beacon in MANET using DSR. Apart from this, the prominent dependency in DSR is to ensure all symmetric links find the route based on the header information. In case of faulty transmission, DSR protocol initiates maintenance, allowing the mobile node to generate error routes packets. This eliminates faulty links from the cached information, resulting in truncating all the faulty links generated from that mobile node. The updated routes are explored using the route discovery stage. Hence, to formulate a robust, secure strategy, it is necessary to realize the strength and weaknesses of the conventional DSR scheme in MANET. Realization of weakness will better formulate a proposed security solution that balances communication and security performance. The beneficial aspects of the DSR protocol are its adoption of an on-demand scheme that doesn't have any dependency on the regular transmission of update messages not to flood the network. The construction of the routes in DSR is carried out only when required, allowing the security system to monitor the threat closely. DSR significantly reduces the control overhead by ensuring utilization of route cache information by the relay node in MANET, which will be an added advantage towards supporting security operation. However, there are various discrepancies towards deploying conventional DSR in its actual form in security. The primary security challenge in DSR is that the broken link is not locally repaired while performing maintenance tasks, which attracts intrusion towards this broken link. The secondary security challenge in DSR is the prevalence of stale cached information of the route that results in critical inconsistencies while formulating new routes. This problem will render the attacker using the close information and intruding on the network during the route reconstruction phase. The tertiary security challenge in DSR is that it has good supportability for the environment with the static and lower extent of mobility; it is not eventually meant to resist security threats in increasing mobility environment. This could also result in potential delay and routing overhead. Hence, the proposed scheme assists in overcoming this pitfall of conventional DSR to mitigate a higher degree of threats in the MANET environment.

In the proposed scheme exhibited in Fig. 3, a novel mechanism is designed that lets all the mobile nodes carry out communication and identification of threats followed by resisting them simultaneously. The novelty of this scheme is to resist attacker nodes by deviating them in counterfeited routes which are applicable for multiple attackers of dynamic form in MANET. Unlike existing security approaches, the proposed system of DSR doesn't use any form of encryption and yet offers better protection with conservation of resources and efforts of mobile nodes towards executing security operations. This model provides counterfeited route information as the mitigation solution towards resisting attackers in MANET.

B. Proposed Enhanced DSR Implementation

The proposed system incorporates a certain degree of novelty to address the three essential loopholes discussed in the prior section in the DSR protocol. This is carried out towards strengthening DSR protocol for making it a high potential for identifying and mitigating threats. Following are the set of novel features introduced in the proposed secure DSR implementation in the MANET environment:

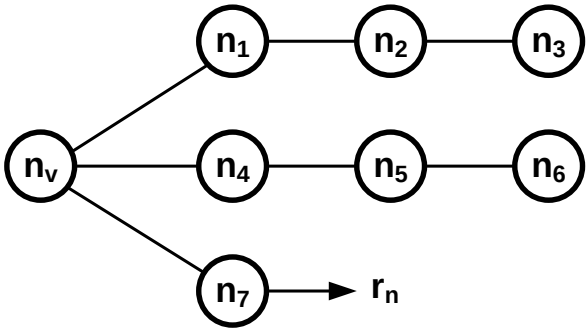

Fig. 3. Mechanism of Proposed DSR Scheme.

- The proposed model doesn't depend on any trusted third party or any other centralized scheme using DSR protocol.
- Unlike the existing DSR protocol, the proposed secured DSR protocol will assess the integrity by computing the inconsistency between the defined MANET topology and HELLO message.
- The proposed study appoints a specialized mobile node called an auxiliary relay node responsible for the broadcasting HELLO message and has the privilege to alter the topology to ensure faster route-finding towards the destination. Hence, the idea is also to protect this auxiliary relay node from threats.
- If there is no inconsistency, the model selects a single auxiliary relay node. However, in case of contradiction, the auxiliary relay node can be elected for all double-hop neighboring nodes where the auxiliary node plays the role of the single access point. However, neighboring nodes in double-hop with other paths are not privileged to select as a particular auxiliary relay node.

The properties mentioned above are incorporated within the DSR protocol. The prime justification of the above points is as follows: in case of any unknown attack, the initiation point will always be from the topology control message introduced in the proposed system. Eventually, it is impossible to stop the attacker (or vulnerable mobile node) from propagating legitimate control messages for topology control. Suppose the attacker broadcasts a counterfeited control message that eventually declares his presence, leading other mobile nodes to safeguard themselves. Therefore, a counterfeited control message is potentially a prominent strategy for the attacker. It can isolate the vulnerable node from the network entirely without the vulnerable node knowing about it. So, the idea of the proposed secure DSR protocol is to present a solution towards misleading the attacker node by using a retaliation node. In this case, the retaliation node will present a series of counterfeited information of node address to attacker or victim node once identified. The attacker/victim node will comply with the proposed protocol and will not deny the list of routes they are supposed to traverse. This will lead to the attacker node utilizing all its resources to find the counterfeited nodes, and this process will continue until they expend all its resources. After delivering the address list to attackers, the retaliation node is eliminated, and hence the network is fully secured even if the attacker changes its strategy. The following section discusses algorithm implementation as a part of the proposed solution.

C. Algorithm Design

This algorithm is responsible for determining the unknown threat present in the MANET environment. The complete discussion of the algorithm is carried out, referring to Fig. 3. The parameters used by the algorithms are i) mobile nodes V, ii) vulnerable node nv, which are part of normal mobile nodes V, iii) retaliation node rn that is advertised by node n7, iv) single and multihop neighboring nodes, i.e., sh(nv) and mh(nv) respectively, v) primary auxiliary relay node aux(nv) that maintains series of single-hop nodes of nv who elected nv as their auxiliary relay node, vi) secondary auxiliary relay node aux_sh(nv) which is a series of single-hop mobile nodes that are elected by the nv as the primary auxiliary node. The steps of the algorithm are as follows:

Algorithm for Determining the Threat

Input: *N* (mobile nodes)
Output: *b* (determining the state of threat)
Start
1. **For** i=1:N
2. $n_7 \rightarrow f_1$("HELLO||sh(n_v,n_2,n_5,r_n)")
3. n_v confirms (f_1(HELLO)||exclude(sh(n_v)))
4. **For** j=1:k
5. **If** Δ=1
6. **For** Δ≠g(HELLO)
7. **For** Δ≥dist(mh(n_v))
8. **If** n7→elect[λ(sh(n_v))]
9. nv checks Δ
10. n7 elects Δ
11. else
12. b=Δ elects n7 as aux_node
13. **End**
14. **End**
15. **End**
16. **End**
End

This algorithm assesses the control message disseminated by the mobile node in MANET using the proposed secured DSR protocol. Referring to Fig. 3, the algorithm considers single and multihop nodes of vulnerable mobile node nv as,

$$sh(n_v)=\{n_1, n_4, n_7\}$$

$$mh(n_v)=\{n_2, n_5\} \quad (1)$$

According to the proposed system, the vulnerable node nv should elect a secondary auxiliary relay node aux_sh(nv) which is a matrix retaining information about first-hop node n1 and n4; this is done by proposed secured DSR so that it can protect the request propagation to multihop nodes, i.e., mh(nv) which retains information about neighboring nodes of nv. Therefore, in the presence of the unknown adversary, the mobile node n7 will advertise a counterfeited control message which consists of single-hop information, i.e., sh(nv) consists

of vulnerable node nv and multihop nodes (n2, n5) and node n7(Line-1). However, the proposed system will not allow announcingn1 and n2 as it is possible for nv to validate this by considering the control message (HELLO) of node n7 with the control message of node n1 and n4. So, the proposed algorithm set up a protocol which is as follows: the vulnerable node nv should confirm that the announced mobile node by it should not match with the elements of matrix storing single-hop node information of vulnerable node sh(nv) (Line-3). This operation is carried out during the announcement of the control message by node n7, which possesses information about single-hop node information of n7.

On the other hand, node n7 should opt for an auxiliary relay node that will permit the usage of n1 and n4 (as they will be present in matrix storing mh(n7)). As a security mechanism, node n7 will falsely act as it opts for vulnerable node n7 as an auxiliary relay node to encapsulate its single-hop nodes n1 and n4. According to the proposed algorithm, the vulnerable node nv cannot infer that node n7 is an attacker. On the other hand, the vulnerable node nv can assess if the node n7 selects some of the auxiliary relay nodes for encapsulating multihop nodes of n7, i.e., mh(n7) with single-hop nodes of vulnerable node, i.e.,n1 and n4, i.e., It will eventually mean to assess the target node as n2 and n5 to be protected. Hence, the proposed algorithm set up another protocol that states: For a target k mobile node included within a control message (Line-4), the vulnerable node nv assesses the presence of another node Δ which are the subset of single-hop neighboring nodes of k (Line-5). The unit value in Line-5 represents the binary condition of its presence. Apart from this, the algorithm also ensures that Δ is not present in the sender's control message using a search function g(x) (Line-6). It also checks if Δ is positioned at a distance dist of multiple hops (at least three hops) (Line-7). The study analyzes another assessment to match this condition to determine if node n7 has elected λ mobile node (Line-8), which is also a part of single-hop neighboring nodes of n7 as the auxiliary node for encapsulating Δ (Line-9). This is followed by the election of Δ by node n7 (Line-10). Otherwise, the algorithm lets Δ elect n7 as the auxiliary node (Line-12). The above-stated operation can be carried out by searching within the routing table consisting of topology control information. Apart from this, it is feasible for the attacker to bypass this security scan by announcing that its position is in single hope from all the nodes N. Hence, to mitigate this challenge, the proposed system considers vulnerable node nv to possess conflicting and susceptible control messages consisting of all single-hop neighboring nodes of it. The algorithm mentioned above is meant to execute the mentioned rules sequentially to determine the state of intrusion, determined by variable b (Line-12). In case of any conflict, the vulnerable node nv elects n7 as the only auxiliary relay node exclusively for the mobile nodes that are announced the control message of node n7. Hence, the proposed algorithm without including any conventional encryption approach or complex iterative approach, the proposed algorithm can trace out the potential malicious behavior of an unknown attacker in MANET.

The next part of the algorithm implementation is towards resisting intrusion in MANET using the proposed secured DSR protocol. In this algorithm, the retaliation node is designed, responsible for forwarding counterfeited node information to the attacker once the attacker is positively identified in the prior algorithm. The steps of the algorithm are as follows:

Algorithm for resisting attack

Input: r_n (retaliation node)
Output: C (forwarding counterfeited route)
Start
1. $\Delta \rightarrow$add (r_n) for rn$\notin$sh(nv)
2. **If** Step-1=True
3. Δ broadcast r_n and compute aux_{prob}
4. **If** aux_{prob}=false
5. remove r_n
6. **End**
7. Compute outlier
8. C: $r_n \rightarrow f_2$(attacker)

End

The retaliation node is defined by Δ, which doesn't exist in the real-time MANET environment to mislead the attacker. In this case, the node Δ adds a retaliation node such that they don't belong to a class of single-hop neighboring nodes of vulnerable node nv (Line-1). All the new nodes Δ announce and advertise the information of the retaliation node if the first step is valid (Line-2). Further, it also computes the probability of auxiliary relay node (Line-3) considering all the mobile nodes concerning single-hop neighboring nodes of vulnerable node nv. When the probability computation for the auxiliary relay node is false (Line-4), the retaliation node rn is removed (Line-5). There is a benefit for this step, as after the retaliation node offers information of counterfeited nodes that don't exist to the intruder, the retaliation node must be eliminated. This will remove all the possibilities of intruders attempting to understand the strategy of proposed mitigation measures.

Further, the algorithm will compute outliers, calculated by calculating a total number of vulnerable nodes positively identified divided by a single hop neighborhood of vulnerable node nv (Line-7). In this case, the probability is computed for arbitrarily selected mobile nodes that are wrongly designated as an attacker, leading to vulnerable node nv preventing it as its auxiliary relay node. Hence, the system computes the possible distrusted mobile node to be part of vulnerable node nv, and it is a subset of single-hop neighboring nodes of nv. Then, the algorithm formulates a data transmission function f2(x) that advertises some randomly selected nodes that are not the common node to the attacker (Line-8). Upon receiving this information, the attacker will need to trust the data and select the routing towards the counterfeited path C leading to complete energy drainage. This mechanism doesn't lead to any form of halt in the communication system of regular nodes. The novelty of this algorithm is that it doesn't perform any form of iterative operation and offer a dual-layer of checks to confirm the malicious behavior of an unknown mobile node. The following section discusses simulation outcomes obtained by implementing the proposed algorithm.

VI. Result Analysis

The implementation of the proposed logic is scripted in MATLAB. The analysis considers 500-1000 mobile nodes deployed within 1000 x 1000 m2 simulation area. The assessment is carried out for 1000 simulation rounds where the test environment is created for node density while four performance parameters are chosen to be evaluated viz. i) proportion of retaliation node, ii) Throughput, iii) proportion of required Auxiliary Relay Node (ARN), and iv) processing time. The comparison is carried out concerning conventional DSR protocol. The prime justification is that the proposed system offers security by incorporating a series of DSR protocol changes without including any conventional encryption or security system in MANET. This makes it more suitable to be compared with traditional DSR protocol, which lacks any security incorporations.

A. The Proportion of Retaliation Node

The computation of the retaliation node is carried out by consistently monitoring the available number of retaliation modern while implementing the algorithm. Cost effective security solution will anticipate reduced dependencies of retaliation node, which is analyzed in this part of result analysis. The observation is carried out over increasing node density, representing increasing traffic load and an unknown attacker.

Fig. 4 highlights that the proposed system progressively reduces the retaliation node's dependencies, which can be justified as follows: According to the algorithm, the retaliation node doesn't exist in real-time. It only exists in the form of memory which forwards counterfeited information to attackers. Once the attackers comply with its generated path of rn, these memories are disposed of off completely. In case of further attack, the vulnerable node is now aware of the attacker node identity. Hence, without even using the retaliation node, the vulnerable node can isolate themselves from any form of communication (route discovery and data forwarding) and therefore be safe without depending on the retaliation node. Hence, the dependency of rn decreases with the increase of traffic.

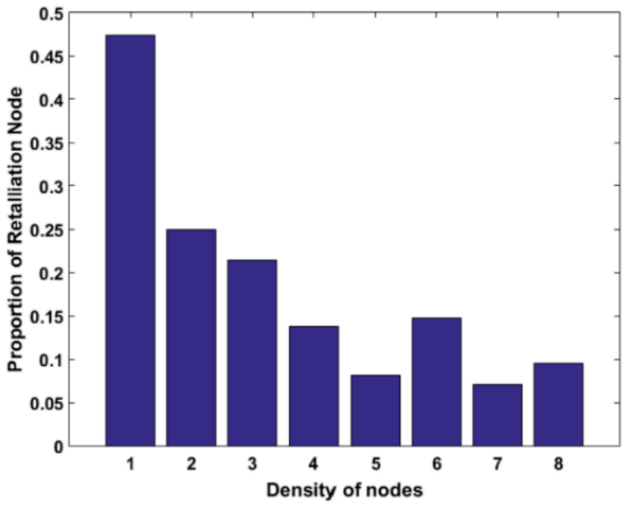

Fig. 4. Proportion of Retaliation Node.

B. Throughput Analysis

The proposed system computes throughput by monitoring the cumulative data received by the destination mobile nodes in the MANET environment measured in kilobytes per second.

The assessment is carried out separately for both DSR and Secured DSR protocol (proposed) in the presence of increasing node density. The outcome exhibited in Fig. 5 highlights that the proposed system offers better throughput than the existing system. The major reason is that conventional DSR protocol suffers from the challenge of retaining stale route information, which causes usage of similar routes for a specific range of data transmission attempts iteratively. In the presence of an attacker, this route is often compromised, leading to lower availability of channel capacity, causing degradation in throughput. On the other hand, the proposed system maintains the parallel process of identification and prevention using retaliation node without any effect on ongoing communication. This causes the proposed method to be less sensitive towards an attacker's presence once they are positively identified.

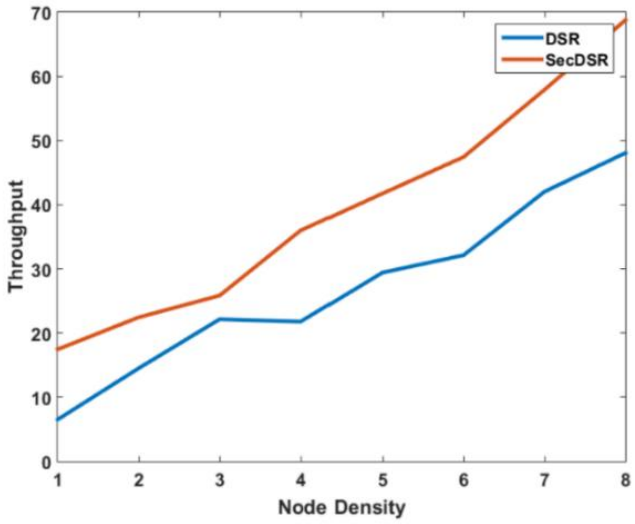

Fig. 5. Proportion of Throughput.

C. The Proportion of Required ARN

Auxiliary Relay Node (ARN) plays a contributory role in the proposed study. It holds the responsibility of route discovery for data transmission and topology management in case of the attacker's presence in the proposed DSR protocol. However, it should also be noted that there is no physical presence of a retaliation node in the proposed system. In contrast, ARN has a physical presence in the specially selected node based on the highest resource contents. All work carried out in MANET only uses mobile nodes, whereas the proposed system uses mobile nodes and ARN as a novelty. So it is wise enough to find out if such an ARN node affects the network with an increasing traffic load. For the system to be more secure, it is required to reduce the number of ARN with increasing traffic as the privilege of ARN to control topology is a prime attempt to be compromised by the attacker. Fig. 6 highlights that the proposed system offers significantly fewer ARN nodes in comparison to the existing DSR. The DSR protocol does not include the ARN concept; however, to

maintain a similar testbed, analysis is carried out to find the impact of the presence of ARN in regular DSR operation and proposed secured DSR operation. The calculation is carried out by monitoring a total number of instantaneous selected ARN during each iteration corresponding to node density. The prime justification behind this outcome is that: conventional DSR protocol uses source routing where there is a dependency toward retaining node address within the routed packet.

Further, the cached information of DSR keeps on increasing with increasing node density. So, technically DSR protocol doesn't offer much supportability towards the proposed usage of ARN. However, due to the formulated operation of the proposed algorithm with ARN, conventional DSR is found to be better when ARN is used. The proposed system further exceeds this outcome as ARN is selected only when a significantly new topology of MANET is encountered. The proposed method also keeps on computing outliers, ensuring that the detection rate is always higher, reducing dependencies on ARN.

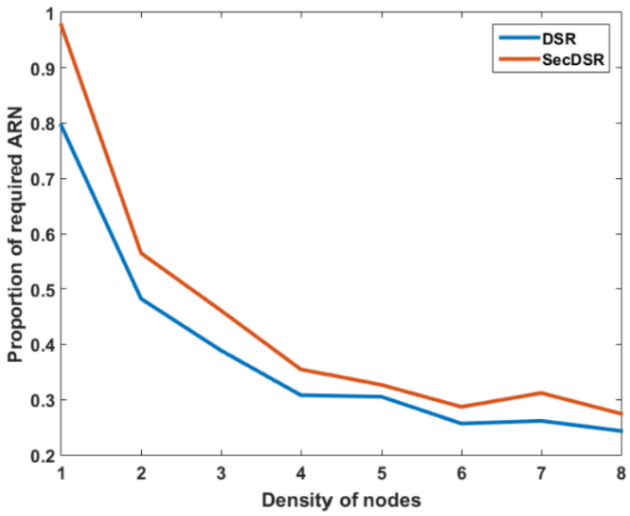

Fig. 6. Proportion of Required ARN.

D. Processing Time

Cumulative time required to execute the algorithm gives processing time, as exhibited in Table I.

TABLE I. ANALYSIS OF PROCESSING TIME

	DSR	SecDSR
Processing Time	8.825 s	1.271 s

The prime reason behind reduced processing time for the proposed system (SecDSR) is because it doesn't have an inclusion of much iterative operation concerning route discovery, maintenance, intrusion detection, and prevention as compared to existing DSR where higher iterative and more operative steps in involved to find the effective routes of communication in MANET environment. This causes reduced time for the proposed system in contrast to conventional DSR.

VII. DISCUSSION

From the prior section, it has been seen that proposed system carries out better performance outcome in contrast to existing secured DSR version. Following are the learning outcomes extracted from this model implementation:

- The proposed scheme is highly suitable for application working on WANET which is basically larger in dimension as well as distributed. This is because of the memory sharing concept by each nodes where updating the threat flags are quite faster compared to conventional DSR. Therefore, a better processing time is obtained.
- The proposed system ensures its applicability of dynamic attacker as well as multi-attacker at same time. It is because it can formulate an assessment with respect to unit hop link associated with the legitimacy of the attacker node. Hence, any node changes its strategy at any point of time will be instantly notify the other nodes about this chance. This causes faster identification of attack environment.
- The throughput of proposed system is quite good and this is because of the non-inclusion of iterative checks or sophisticated classes of operation. Along with assessing the legitimacy of the nodes, the prime target node can always perform seamless propagation of data to its destination node. Hence, data propagation is not affected by its assessment process towards intrusion.

Therefore, on the above ground of constructive outcome, it can be stated that proposed system offers a simplified and cost efficient computational solution towards securing WANET from potential threats.

VIII. CONCLUSION

The proposed system approaches resisting unknown attackers in MANET based on computation being carried out on malicious behavior. In the adversary, the study considers that the vulnerable node is manipulated by the attacker while playing the role of the auxiliary relay node. By doing this, the adversary will be able to gain access to the complete network. The proposed system offers a solution to resist it. The contribution of the proposed study is as follows:

- The proposed model assists in safeguarding the routes as well as nodes connected in MANET from being disclosed to the adversary without any form of dependencies of any trusted authority or third party.
- The proposed model introduced an auxiliary relay node which is responsible for performing route discovery as well as management of topology which reduces the same effort carried out by mobile nodes as seen in the existing system.
- The proposed method introduces a retaliation node which is a non-physical entity to mislead the attacker as a unique prevention strategy unlike any current mechanism in MANET.

The future work of the proposed system will be carried out further to optimize the study outcomes. Adoption of bio-inspired protocols can be adopted in order to find out more optimized solution towards delay and data propagation. More cases of multi-objective function can be formulated to ensure more resistivity towards physical attacks.

REFERENCES

[1] K. -H. Cho, S. -H. Lee and V. Y. F. Tan, "Throughput Scaling of Covert Communication Over Wireless Adhoc Networks," *IEEE Transactions on Information Theory*, vol. 66, no. 12, pp. 7684-7701, Dec. 2020, doi: 10.1109/TIT.2020.3011895.

[2] B. Ojetunde, N. Shibata and J. Gao, "Secure Payment System Utilizing MANET for Disaster Areas," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 49, no. 12, pp. 2651-2663, Dec. 2019, doi: 10.1109/TSMC.2017.2752203.

[3] X. Chen, T. Wu, G. Sun and H. Yu, "Software-Defined MANET Swarm for Mobile Monitoring in Hydropower Plants," IEEE Access, vol. 7, pp. 152243-152257, 2019, doi: 10.1109/ACCESS.2019.2948215.

[4] H.S. Bedi, S. Verma, M. Goel, "A Survey on MANET Security Challenges, Attacks and its Countermeasures", *International Journal of Advanced Research in Computer and Communication Engineering*, vol.5, Iss.8, 2016.

[5] K. Kumar, S. Verma, Kavita, NZ Jhanjhi, M N Talib, "A Survey of The Design and Security Mechanisms of The Wireless Networks and Mobile Ad-Hoc Networks", *OP Conf. Series: Materials Science and Engineering*, vol.993 2020.

[6] M. S. Khan, D. Midi, M. I. Khan, and E. Bertino, "Fine-Grained Analysis of Packet Loss in MANETs," *IEEE Access*, vol. 5, pp. 7798-7807, 2017, doi: 10.1109/ACCESS.2017.2694467.

[7] Motwani and Anand, "Survey of Malicious Attacks in MANET", *International Journal of Computer Applications*, vol.80, pp.28-30, 2013. Doi 10.5120/13931-1916.

[8] Bhatia, Tarunpreet & Verma, A., "Security Issues in Manet: A Survey on Attacks and Defense Mechanisms", *International Journal of Advanced Research in Computer Science and Software Engineering*, vol.3, pp.1382-1394, 2013.

[9] F. Abdel-Fattah, K. A. Farhan, F. H. Al-Tarawneh and F. AlTamimi, "Security Challenges and Attacks in Dynamic Mobile Ad Hoc Networks MANETs," *IEEE Jordan International Joint Conference on Electrical Engineering and Information Technology*, pp. 28-33, 2019, doi: 10.1109/JEEIT.2019.8717449.

[10] G. Toso, R. Masiero, P. Casari, M. Komar, O. Kebkal and M. Zorzi, "Revisiting Source Routing for Underwater Networking: The SUN Protocol," IEEE Access, vol. 6, pp. 1525-1541, 2018, doi: 10.1109/ACCESS.2017.2779426.

[11] R. Abassi, A. B. C. Douss, & D. Sauveron, "TSME: a trust-based security scheme for message exchange in vehicular Ad hoc networks" *Springer Open-Human-centric Computing and Information Sciences*, Article No.43, 2020.

[12] J. Chen, T. Li, and J. Panneerselvam, "TMEC: A Trust Management Based on Evidence Combination on Attack-Resistant and Collaborative Internet of Vehicles," *IEEE Access*, vol. 7, pp. 148913-148922, 2019, doi: 10.1109/ACCESS.2018.2876153.

[13] L. Guaya-Delgado, E. Pallarès-Segarra, A. M. M. & J. Forné, "A novel dynamic reputation-based source routing protocol for mobile ad hoc networks", *Springer-EURASIP Journal on Wireless Communications and Networking*, Article No. 77, 2019.

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

[15] J. V S & Manikandan M S K, "Efficient trust management with Bayesian-Evidence theorem to secure public-key infrastructure-based mobile ad hoc networks", *Springer-EURASIP Journal on Wireless Communications and Networking*, Article number: 25, 2018.

[16] N. I. Mowla, N. H. Tran, I. Doh and K. Chae, "Federated Learning-Based Cognitive Detection of Jamming Attack in Flying Ad-Hoc Network," *IEEE Access*, vol. 8, pp. 4338-4350, 2020, doi: 10.1109/ACCESS.2019.2962873.

[17] M. S. Khan, M. I. Khan, Saif-Ur-Rehman Malik, Osman Khalid, Mukhtar Azim & Nadeem Javaid, "MATF: a multi-attribute trust framework for MANETs", *Springer- EURASIP Journal on Wireless Communications and Networking*, Article number: 197,2016.

[18] T. Kavitha & K. Geetha & R. Muthaiah, "India: Intruder Node Detection and Isolation Action in Mobile Ad Hoc Networks Using Feature Optimization and Classification Approach", *Wiley-Journal of Medical Systems*, vol.43, Iss.179, 2019.

[19] M. Faisal, S. Abbas & H. Ur Rahman, "Identity attack detection system for 802.11-based ad hoc networks", *EURASIP Journal on Wireless Communications and Networking*, Article number: 128, 2018.

[20] 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*, Article number: 52, 2021.

[21] A. Yasin and. A. Zant, "Detecting and Isolating Blackhole Attacks in MANET Using Timer Based Baited Technique", *Wiley-Hindawi Wireless Communications and Mobile Computing*, 2018.

[22] T. A. Alghamdi, "Convolutional technique for enhancing security in wireless sensor networks against malicious nodes", *Human-centric Computing and Information Sciences*, vol.9, Article number: 38,2019.

[23] Y. Wang, M. Zhang & W. Shu, "An emerging intelligent optimization algorithm based on trust sensing model for wireless sensor networks" *EURASIP Journal on Wireless Communications and Networking*, Article number: 145, 2018.

[24] S. A. Almazok & B. Bilgehan, "A novel dynamic source routing (DSR) protocol based on minimum execution time scheduling and moth flame optimization (MET-MFO)", *EURASIP Journal on Wireless Communications and Networking*, vol.2020, Article number: 219, 2020.

[25] S. Begum, Y. Nianmin, S. B. H. Shah, A. Abdollahi, "Source Routing for Distributed Big Data-Based Cognitive Internet of Things (CIoT)", *Wiley-Hindawi Wireless Communications and Mobile Computing*, 2021.

[26] F. Ishmanov and Y. B. Zikria, "Trust Mechanisms to Secure Routing in Wireless Sensor Networks: Current State of the Research and Open Research Issues", *Hindawi-Journal of Sensors*, 2017.

[27] H. Kojima, N. Yanai, and J. P. Cruz, "ISDSR+: Improving the Security and Availability of Secure Routing Protocol," in IEEE Access, vol. 7, pp. 74849-74868, 2019, doi: 10.1109/ACCESS.2019.2916318.

[28] Q. Liang, T. Lin, F. Wu, F. Zhang, W. Xiong, "A dynamic source routing protocol based on path reliability and link monitoring repair", *PLOS ONE, Open Access*, 2021.

[29] M. Mohanapriya, N. Joshi, M. Soni, "Secure dynamic source routing protocol for defending blackhole attacks in mobile Ad hoc networks", *Indonesian Journal of Electrical Engineering and Computer Science*, Vol. 21, No. 1, pp. 582~590, 2021.

[30] A. Srivastava, S. K. Gupta, M. Najim, N. Sahu, G. Aggarwal & B. D. Mazumdar, "DSSAM: digitally signed secure acknowledgement method for mobile ad hoc network", *EURASIP Journal on Wireless Communications and Networking*, vol.2021, Article number: 12, 2021.