IJIRSET
International Journal of Innovative Research in
SCIENCE | ENGINEERING | TECHNOLOGY

e-ISSN: 2319-8753 | p-ISSN: 2347-6710

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 11, Special Issue 1, April 2022

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.118

9940 572 462 | 6381 907 438 | ijirset@gmail.com | www.ijirset.com

ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology
An ISO 3297: 2007 Certified Organization Volume 11, Special Issue 1, April 2022
9th National Conference on Frontiers in Communication and Signal Processing Systems (NCFCSPS '22)
28 th -29 th April 2022
Organized by
Department of ECE, Adhiyamaan College of Engineering, Hosur, Tamilnadu, India

An Active-Routing Authentication Scheme in MANET

K.Rajesh Kumar[1], S.Sunil Kumar[2], G.Thirumal[3], R.M Yuvan[4], S.Balachandran[5]

Assistant Professor, Department of Electronics and communication Engineering, Adhiyamaan College of Engineering, Krishnagiri District, Tamil Nadu, India[1]

U.G. Students, Department of Electronics and Communication Engineering, Adhiyamaaan College of Engineering, Krishnagiri District, Tamil Nādu, India[2,3,4,5]

ABSTRACT : Mobile ad-hoc networks (MANET) is a network mode that does not depend on network infrastructure and central access. The fast and flexible networking mode of MANET renders its wide applications in specific scenarios. However, rapidly changing topology and open channels bring potential security problems. In this paper, we proposed an active-routing authentication scheme (AAS) based on the characteristics of active routing protocols. We formally demonstrated that the AAS is effective against selective forwarding attack, false routing attack, byzantine attack and route spoofing attack using the BAN logic considering the possibility of malicious nodes mingling in MANET. Experimental results show that the AAS is compatible with multiple active routing protocols and it is able to increase the packet delivery rate by 33.9%, with an average increase of 18.4% in the network containing some malicious nodes. Furthermore, the AAS is robust which remains the average network connection rate reach 1.6 times of the collusion attack prevention-OLSR(Cap-OLSR) protocol and preserves 79.2% of the network performance in simulation experiments with attacks from malicious nodes.

KEYWORDS : Mobile ad-hoc network, active routing, authentication scheme, secure

I. INTRODUCTION

Mobile ad-hoc networks (MANET) [1] is a self-configuring wireless network consisting of wireless devices with mobility. MANET has the characteristic of minimal configuration and rapid deployment, which is suitable for emergency situation scenarios such as natural disasters, military conflicts and emergency medical care, etc. Due to the characteristics of network and application scenarios, the topology of MANET is variable and unpredictable, bring great challenges to secu- rity [2]. In MANET, traditional security measures are no longer effective. Various attack behaviors, such as, selective forwarding attack, false routing attack, byzantine attack and so on cause the security problems of MANET increasingly prominent. Active routing protocols [3], also known as table-driven routing protocols or prior routing protocols, are based on the principle that each node maintains a routing table that con- tains routing information for all reachable nodes in the net- work. A node obtains the route to the destination by looking up the routing table immediately for sending messages with few delays.

Active routing protocols periodically maintain the topol- ogy of the network and update routing information, relying on the perception of local topology changed by nodes. Each node can periodically broadcast the HELLO message. The time to live (TTL) of the message is set to 1, so that the message cannot be forwarded. The node maintains its neighbor list by receiving the HELLO messages. When the source node of the HELLO message is not in the neighbor list, it indicates that a new node has joined the local topology. And when the node cannot receive the HELLO message sent by a neighbor node periodically, it means that the neighbor node has exited local topology. When nodes in the network sense the change of local topology information, they will reflect the change to the entire network in time by broadcasting the topology control

ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology
An ISO 3297: 2007 Certified Organization Volume 11, Special Issue 1, April 2022
9th National Conference on Frontiers in Communication and Signal Processing Systems (NCFCSPS '22)
28 th -29 th April 2022
Organized by
Department of ECE, Adhiyamaan College of Engineering, Hosur, Tamilnadu, India

(TC) messages. After that, nodes will recalculate the routes to other nodes based on the updated topology information and the routing algorithm agreed in advance. Common active routing protocols, such as Optimized Link State Routing Pro- tocol (OLSR) and Destination-Sequenced Distance Vector Protocol (DSDV) [4], use the above mechanism to update routing information.

In the actual environment, it is necessary to set the network number for the nodes. Nodes with the same network number will automatically join the same network.. In order to ensure the security of networks, a node, which is about to join the network, needs to pass the verification of authentication algorithms at first. If the authentication failed, in principle, the node should not communicate with other nodes in the network and participate in the construction of the network topology. In the viewpoint of the active routing protocol, nodes that are configured for the network have no difference from others. It means that the failure of the authentication algorithm cannot affect the routing protocol's behavior on the node. The unauthenticated node is able to play the same role as other authenticated nodes in the network topology main- tained by the routing protocol, for instance, acting as a hop on communication routes. Unless the unauthenticated node actively moves away from the network, the impact on other nodes in the network is inevitable. Therefore, in MANET with active routing protocols, it is a challenge to prevent nodes that does not pass the authentication from affecting the construction of topology and routing table of the network.

II. RELATED WORK

A lot of research literature is working on the MANET secu- rity issue. There are two categories can be separated from these articles. One focuses on increasing the confidentiality of information such as network topology and data transmis- sion to protect against external attacks. Zhang *et al.* [5] pro- pose the topology-hiding multipath routing protocol TOHIP for the problem of topology exposure in multipath routing protocols. The protocol does not include link connection information in the routing information, thereby avoiding malicious nodes inferring the network topology by captur- ing the routing information, ensuring the confidentiality of the network. When there is no attack, the TOHIP proto- col maintains normal route lookup performance, and in the presence of the attack, TOHIP resists the attack with lower overhead and shorter route convergence time. Rahman and Mahi [6] propose a hybrid Adhoc routing protocol based on the zone routing protocol(ZRP), Secure Zone Routing Proto- col(SZRP). The SZRP protocol integrates digital signatures and asymmetric encryption algorithms through advanced security techniques such as SHA-256, HMAC and pbkdf2 to ensure the security of data transmission in the network. In [7], a heuristic algorithm is proposed to find the safest path from the source UAV to the destination UAV. These algorithms do not remove malicious nodes from the network, so they can still participate in the construction of the network.

The other pays attention on the node authentication algo- rithm for trusted routing to defend against some internal attack. Eirefaie *et al.* [8] make improvements to the ZRP protocol against packet loss attacks, using the concept of trustworthiness to detect packet loss attacks by nodes. After sending a data packet to the neighbor node, the node keeps a copy of the packet and sets a timer to monitor the behavior of the neighbor node. If the neighbor node completely forwards the data packet within a certain period of time, the node is considered to be performing well and the confidence value is raised. Otherwise, it is considered that the neighbor nodes with malicious behavior will reduce the trust value. Within an updated interval of trust value, when the number of lost data packets exceeds the predefined threshold, the node is identi- fied as a malicious node. Trust-based ZRP protocol selects the most reliable and safe route to the destination by trust value of node. Yi *et al.* has presented the security-aware ad-hoc routing (SAR)method (SAR) [9]. The classification of nodes by SAR scheme depends on the trust level of nodes. This happens by sharing the secret group key for the nodes under same classification. The source node S should ensure the basic necessary security during the process of route discovery. This is done with the help of the element in the path followed during routing between source S and destination D. This men- tioned stipulation can be enforced by S by means of the shared key encryption on route request packet using the shared key linked to the respective security level. In spite of the observed merits, shared key method has problems in the SAR approach as the possibility of more malicious agents over other nodes is considered by classifying under high security for accessing to the secret group keys. In [10],there are two measures available for the main node, one is local isolation, and the other is

ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology
An ISO 3297: 2007 Certified Organization Volume 11, Special Issue 1, April 2022
9th National Conference on Frontiers in Communication and Signal Processing Systems (NCFCSPS '22)
28 th -29 th April 2022
Organized by
Department of ECE, Adhiyamaan College of Engineering, Hosur, Tamilnadu, India

to notify the entire network that the malicious node is isolated by the entire network. In Cap-OLSR [11], address of the malicious nodes will be removed from the list of one-hop and two-hop neighbors, causing the node to be isolated from the network. The routing strategy of [12] is to exclude nodes whose trust value is lower than the threshold, and consider that the remaining nodes can constitute a trusted network. Nabou *et al.* [13] propose a new Multi point Relay (MPR) computation in OLSR, MPR can ensure the security of OLSR routing in the process of route construction against single black hole attack. The distributed fuzzy logic module elim- inates the linear nodes of complexity from the Safety Aware Fuzzy Enhanced Ant Colony Optimization (SAFEACO) [14] routing process, resisting black hole, Sybil and inundation attacks at the same time. In [15], it uses two phases to counter malicious Unmanned aerial vehicles (UAVs) attacks. Firstly, they identify and remove malicious UAVs. Secondly, a mobile agent is used to eliminate malicious UAVs. It can ensure the reliability of neighbor UAVs. Above paper ensures the trustworthiness of the nodes forming the route by shield- ing the nodes considered untrustworthy according to some trust mechanism. However, once the malicious node hijacks the normal node and shields the surrounding normal nodes, there will be no node available for routing. Otherwise, these authentication algorithms have high coupling degree with the routing protocol.

III.METHODOLOGY

A. ASSUMPTION

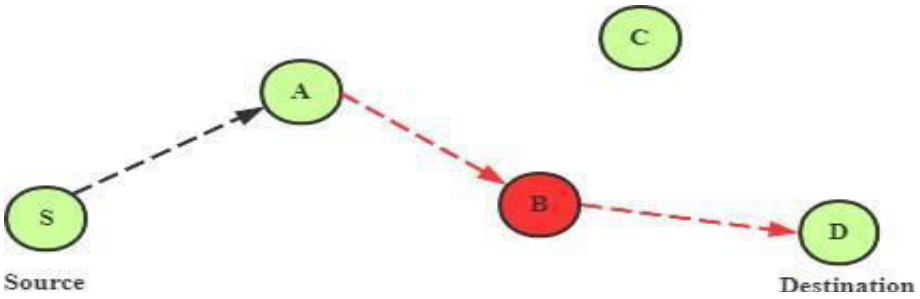
In MANET , some malicious nodes can obtain the network number to join the network and can become authenticated node by hijacking a normal node or exploiting a misjudgment of authentication algorithm. These malicious nodes have the ability to tamper with neighbor node authentication messages, to selectively forward and tamper with passing packets. Malicious nodes are always minority.

B. ATTACK METHODS AND COUNTERMEASURES

1) SELECTIVE FORWARDING ATTACK

A node, as a hop in the communication route of other nodes, which selectively forwards or discards the packets that need to be forwarded. This node can launch selective forwarding attack [16].
The result of the execution of the authentication algorithm does not affect the behavior of the active routing protocol at the node. However, the malicious node still has the opportu- nity to participate in the construction of topology and routing table even if it cannot directly communicate with other nodes in the network without authentication.

As shown in figure 2(a), although node B does not pass the authentication in the communication range of nodes, this node is still selected as a hop of the communication route between node S and node D by active routing protocol. As a result, node B can maliciously attack the passing messages.



ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology
An ISO 3297: 2007 Certified Organization Volume 11, Special Issue 1, April 2022
9th National Conference on Frontiers in Communication and Signal Processing Systems (NCFCSPS '22)
28 th -29 th April 2022
Organized by
Department of ECE, Adhiyamaan College of Engineering, Hosur, Tamilnadu, India

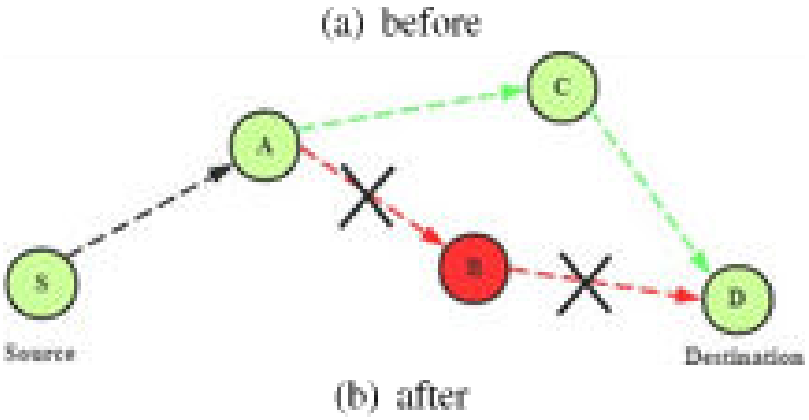


Figure 1. Selective attack example

For the selective forwarding attack, we propose the firewall global shielding strategy. As shown in figure 2(b), assuming that node B fails to pass the authentication launched by node A and node D, and then, node A and node D will set shielding rules about node B according to its IP address and broadcast it to entire network. After receiving the broadcast message, other nodes will also set the same shielding rules. The active routing protocols are aware of the network topology and maintains routing tables by receiving Hello message from neighbor nodes, while firewall can prevent nodes in the net- work receiving Hello messages from unauthenticated nodes. So firewall global shielding strategy can avoid unauthenti- cated nodes participating in the construction of topology and routing. Moreover, this strategy can fundamentally avert the influence of unauthenticated nodes in the network.

2) FALSE ROUTING ATTACK

As shown in figure 3 shown, assuming that node B does not pass the authentication initiated by node M. Node B sends broadcast messages attempting to shield node M before being shielded globally. This mode of attack is called false routing attack [17].

To prevent the false routing attack, we introduced an authenticated node list called A_Set for each node. The A_Set will initialize to the N_Set in section III-B4. When they receive the broadcast message from node B, these nodes will ignore the malicious broadcast message from node B since it is not in A_Set. After that, the malicious shielding attack launched by node B before the shielding rules about node B will be prevented.

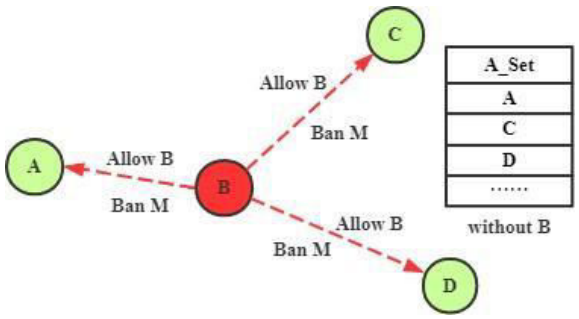


FIGURE 2. False routing attack example

3) BYZANTINE ATTACK

In the network, false-negative nodes will be permanently shielded and unable to join the network again. More seriously, false-positive nodes will maliciously shield other normal nodes which want to join the network by broadcasting the shielding rules. This kind of behavior will produce a large number of false-negative nodes. As a result, there are less nodes available in the network, which eventually brings the network

ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology
An ISO 3297: 2007 Certified Organization Volume 11, Special Issue 1, April 2022
9th National Conference on Frontiers in Communication and Signal Processing Systems (NCFCSPS '22)
28 th -29 th April 2022
Organized by
Department of ECE, Adhiyamaan College of Engineering, Hosur, Tamilnadu, India

to a halt. And we call this attack byzantine att- tack [18]. As shown in the figure (a), node B is a false- positive node. When node C attempts to join the network through node B, node B will maliciously shield node C and force it to be a false-negative node, so that node C cannot join the network normally .

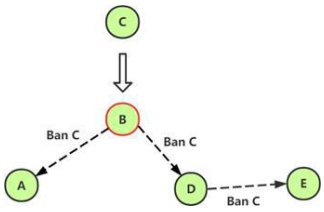


FIGURE 3. Byzantine attack example.

4) ROUTE SPOOFING ATTACK

In figure (a), node B is a false-positive node in the network. When the malicious node C tries to join the network through node B, node B broadcasts a message to the network that node C is authenticated. In this way, the malicious node C be added to the A_Set easily, which will introduce more mali- cious nodes into the network. And we call it route spoofing attack [19].

In response to the route spoofing attack, each node in the network maintains a list of neighbor nodes called N_Set. For each node in the network, once a new node appears in its N_Set, the node will launch the authentication process. Therefore, for false-positive nodes B and C, as long as they appear in the communication range of other trusted nodes, they will be re-authenticate. In this way, there is an oppor- tunity to identify the identity of malicious nodes B and C in the network, so as to resist the routing spoofing attacks of nodes B and C.

C. THE AAS DESIGN

Based on the above analysis, we design the AAS as figure 6. There are three types of broadcast messages that each node may receive related to the AAS: HELLO messages, Shield- ing Node broadcast message, and Node Pass Authentication broadcast message. The processing flow of message (line 4) is shown in algorithm 1.

When node N attempts to join the network, N needs to pass the authentication of nodes in the network which are within the communication range of node N at first. When nodes receive the HELLO message broadcasted from node N, they will detect whether node N is a new neighbor node, and if so, they will initiate the authentication process to node N. The new node of the network may receive authentication requests from multiple nodes at the same time. Set O $o_1, o_2, \ldots o_n$ as the set of nodes that initiate the authentication process to node N, then node N needs to respond to the authentication requests of all nodes in set O (line 2-7). The authentication process is shown in Algorithm 2.

During authentication process, node N is allowed to retry up to $IDENTIFY_{MAX}$ times when it failed in order to avoid accidental factors. $IDENTIFY_{MAX}$ is an empirical value which is set to 3 in our experiments. When node N passes authentication, node o_i will add node N into A_Set and broadcasts Node Pass Authentication message about node N to the network. If node N does not pass authentication within the threshold, node o_i will shield the node N and broadcast Shielding Node message about it.

In addition, as shown in figure 7, the AAS decouples the authentication algorithm from the routing protocol. Active routing protocols provide authentication triggering mecha- nisms to authentication schemes, which provide trusted nodes to routing protocols. The authentication algorithm authen- ticates the node identity, and the communication encryp- tion algorithm provides encrypted secure channel for the authentication scheme. In this way, research on authentica- tion algorithms can focus on itself without

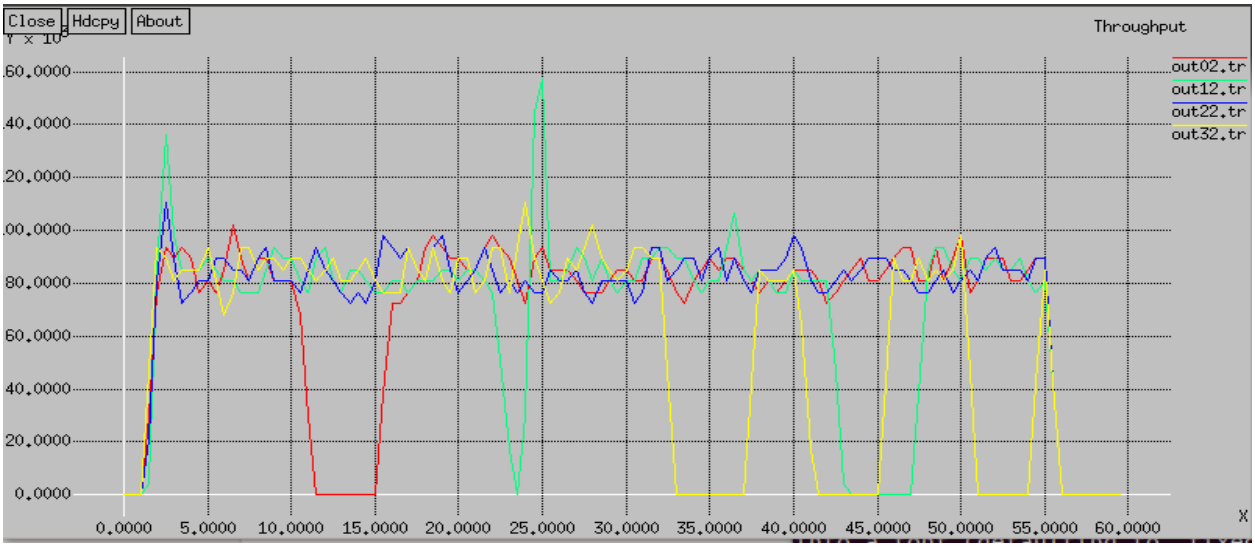
ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology
An ISO 3297: 2007 Certified Organization Volume 11, Special Issue 1, April 2022
9th National Conference on Frontiers in Communication and Signal Processing Systems (NCFCSPS '22)
28 th -29 th April 2022
Organized by
Department of ECE, Adhiyamaan College of Engineering, Hosur, Tamilnadu, India

considering the corresponding routing mechanism. In the worst case, each node in the network needs to execute authentication algorithm $IDENTIFY_{MAX}$ times for m neighbors, which means the time complexity is $O(m\ IDENTIFY_{MAX})$. Because the AAS is based on the active routing protocols, each node needs to maintain the global topological information. In addition, they also need to preserve an A_Set and a N_Set for AAS, so the space complexity is $O(n)$, where n is the capacity of the network.

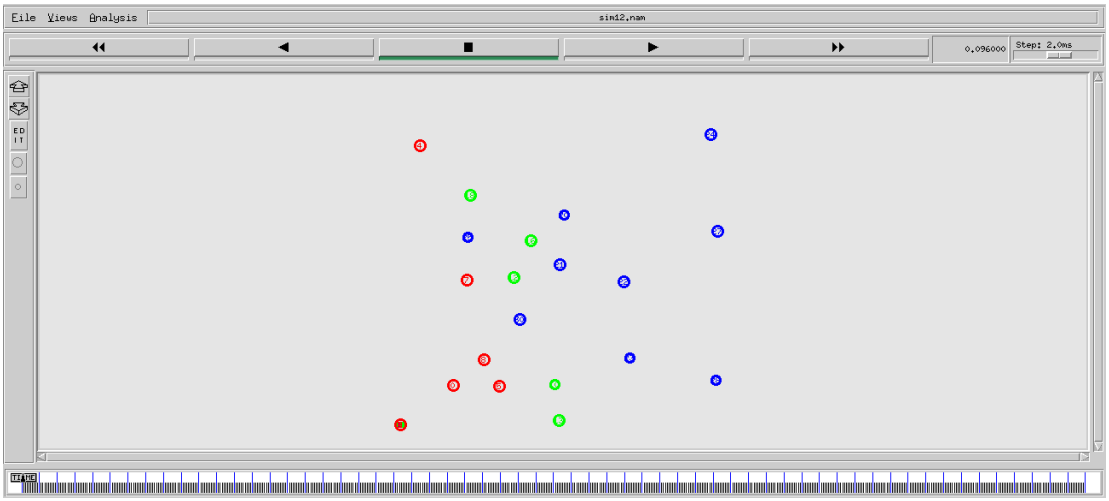
VI. EXPERIMENTAL RESULTS

CONNECTION RATE:



False routing attacks, byzantine attacks, and route spoofing attacks may lead to the reduction of available nodes in MANET and eventually affect the connectivity of the network. In this experiment, we use connectivity as the criterion for validation. The higher the connectivity, the higher the percentage of routes found for the packet to be sent, and the higher the probability of the successful node transmission.

ROUTE SPOOFING ATTACK:

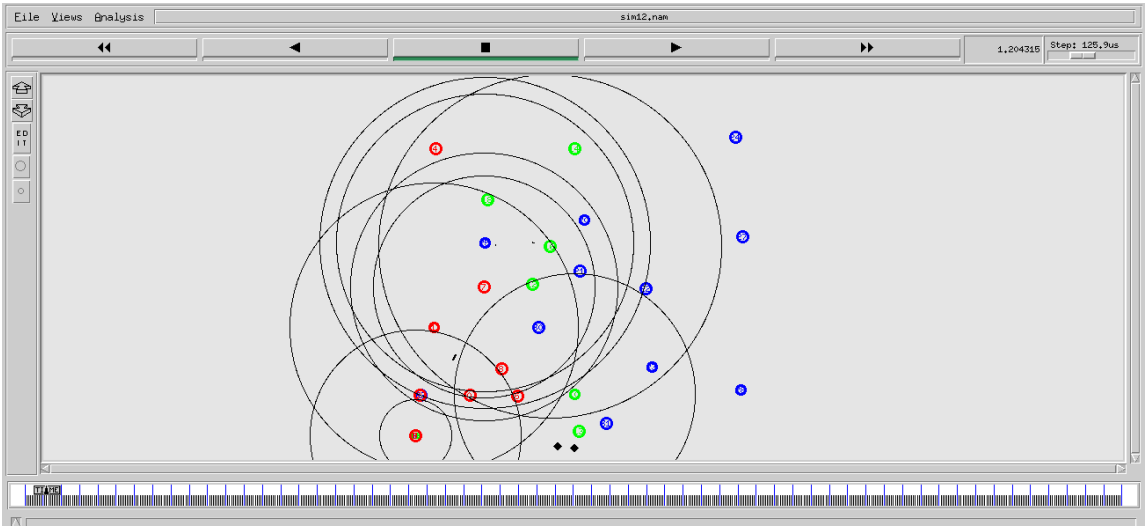


ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology
An ISO 3297: 2007 Certified Organization Volume 11, Special Issue 1, April 2022
9th National Conference on Frontiers in Communication and Signal Processing Systems (NCFCSPS '22)
28 th -29 th April 2022
Organized by
Department of ECE, Adhiyamaan College of Engineering, Hosur, Tamilnadu, India

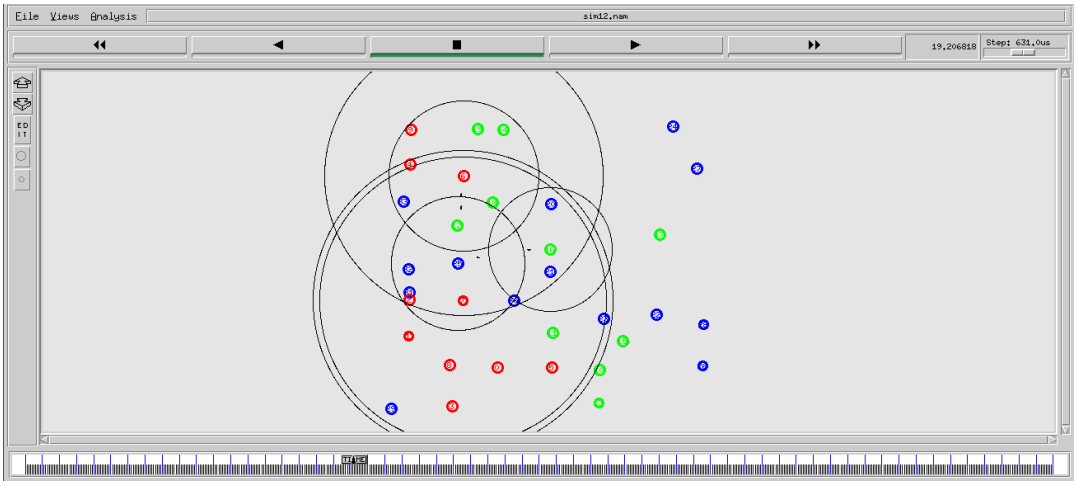
Node B is a false-positive node in the network. When the malicious node C tries to join the network through node B, node B broadcasts a message to the network that node C is authenticated. In this way, the malicious node C be added to the A Set easily, which will introduce more malicious nodes into the network. And we call it route spoofing attack.

Authentication Triggering Mechanisms To Authentication:



Active routing protocols provide authentication triggering mechanisms to authentication schemes, which provide trusted nodes to routing protocols. The authentication algorithm authenticates the node identity, and the communication encryption algorithm provides encrypted secure channel for the authentication scheme. In this way, research on authentication algorithms can focus on itself without considering the corresponding routing mechanism.

ROBUSTNESS MODEL:



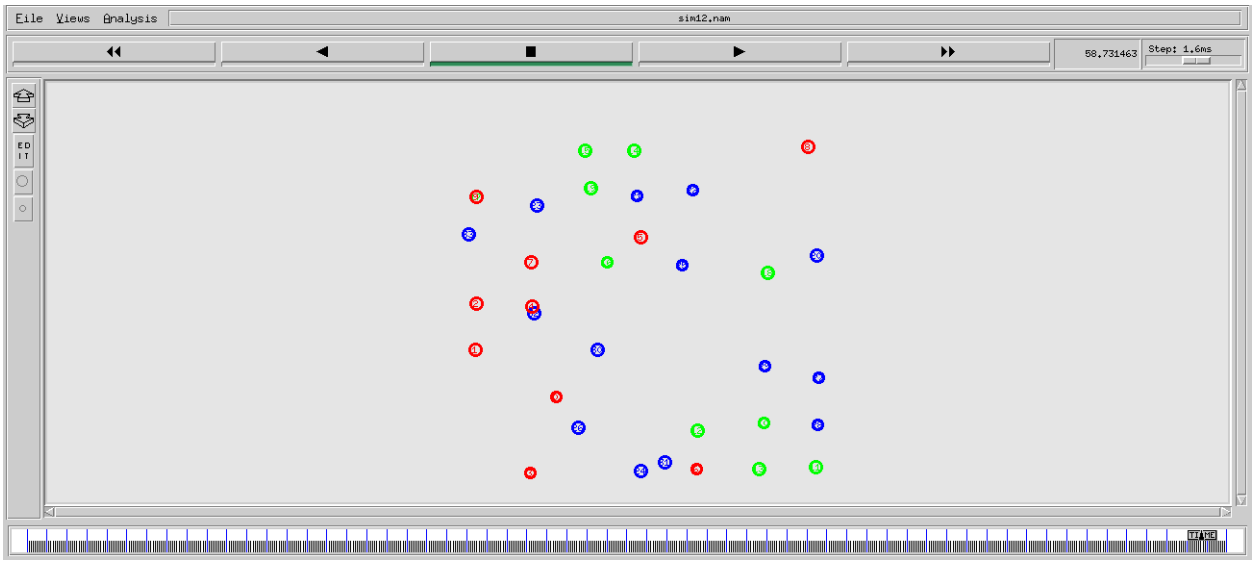
Connectivity determines the successful transmission of data between nodes, while the acquisition of network connectivity is the fundamental guarantee for designing the routing layer. In short, any design of the network is

ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology
An ISO 3297: 2007 Certified Organization Volume 11, Special Issue 1, April 2022
9th National Conference on Frontiers in Communication and Signal Processing Systems (NCFCSPS '22)
28 th -29 th April 2022
Organized by
Department of ECE, Adhiyamaan College of Engineering, Hosur, Tamilnadu, India

based on the assumption that the network is connected. There are many factors that affect connectivity, such as user density, transmit power, channel model, interference, etc.

HYBRID ROUTING PROTOCOLS ANALYSIS:



Three pairs of nodes (source, destination) to communicate, which randomly locate at the initial position of the network. Meanwhile, in order to avoid the influence of accidental factors, we randomly select the malicious nodes which can discard all received packets for each proportion of them. And the average value of multiple experiments are considered as the experimental result. The node movement model is set to Mass Mobility mode, that is, random Waypoint mode, and the node movement speed follows the exponential distribution with the mean value of 10m/s.

V. CONCLUSION

This paper proposes the AAS based on active routing pro- tocols in MANET. The scheme integrates four strategies: firewall strategy, firewall expiration time, authentication node list and neighbor node list. Without relying on authentica- tion algorithms,AAS performs well on resisting the selective forwarding attacks, false routing attacks, byzantine attacks and routing spoofing attacks. Experimental results show that in a network including some malicious nodes, the AAS can increase the packet delivery rate up by 33.9%, with an aver- age increase of 18.4%. At the same time, it can increase the network's connectivity rate to 1.6 times the Cap-OLSR rate under the attacks. In addition, the scheme provides the reference for setting the expiration time in real environment. In future work, we will further investigate the characteristics of reactive routing protocols as well as hybrid routing proto- cols to improve the compatibility of the security authentica- tion scheme for routing protocols, and also we can focus on the other attack modes.

REFERENCES

[1]. N. Khanna and M. Sachdeva, ''BEST: Battery, efficiency and stability based trust mechanism using enhanced AODV for mitigation of blackhole attack and its variants in MANETs,'' Adhoc Sensor Wireless Netw., vol. 46, nos. 3–4, pp. 215–264, 2020. [Online]. Available: https:// www.oldcitypublishing.com/journals/ahswn-home/ahswn-issue-contents/ ahswn-volume-46-number-3-2020/18830-2/
[2]. S. Jamali and R. Fotohi, ''Defending against wormhole attack in MANET using an artificial immune system,'' New Rev. Inf. Netw., vol. 21, no. 2, pp. 79–100, Jul. 2016.

ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology
An ISO 3297: 2007 Certified Organization Volume 11, Special Issue 1, April 2022
9th National Conference on Frontiers in Communication and Signal Processing Systems (NCFCSPS '22)
28 th -29 th April 2022
Organized by
Department of ECE, Adhiyamaan College of Engineering, Hosur, Tamilnadu, India

[3]. M. Boulaiche, ‘‘Survey of secure routing protocols for wireless ad hoc networks,’’ Wireless Pers. Commun., vol. 114, no. 1, pp. 483–517, 2020.
[4]. P. Sarao, ‘‘Comparison of AODV, DSR, and DSDV routing protocols in a wireless network,’’ J. Commun., vol. 13, no. 4, pp. 175–181, 2018.
[5]. Y. Zhang, T. Yan, J. Tian, Q. Hu, G. Wang, and Z. Li, ‘‘TOHIP: A topology-hiding multipath routing protocol in mobile ad hoc networks,’’ Ad Hoc Netw., vol. 21, pp. 109–122, Oct. 2014.
[6]. M. T. Rahman and M. J. N. Mahi, ‘‘Proposal for SZRP protocol with the establishment of the salted SHA-256 bit HMAC PBKDF2 advance security system in a MANET,’’ in Proc. Int. Conf. Electr. Eng. Inf. Commun. Technol., Apr. 2014, pp. 1–5.
[7]. R. Fotohi, E. Nazemi, and F. S. Aliee, ‘‘An agent-based self-protective method to secure communication between UAVs in unmanned aerial vehi- cle networks,’’ Veh. Commun., vol. 26, Dec. 2020, Art. no. 100267.
[8]. Y. Eirefaie, L. Nassef, and I. A. Saroit, ‘‘Enhancing security of zone-based routing protocol using trust,’’ in Proc. 8th Int. Conf. Informat. Syst. (INFOS), May 2012, pp. NW–32–NW–39.
[9]. S. Kianpisheh, N. M. Charkari, and M. Kargahi, ‘‘Ant colony based constrained workflow scheduling for heterogeneous computing systems,’’ Cluster Comput., vol. 19, no. 3, pp. 1053–1070, Sep. 2016.
[10] A. Adnane, C. Bidan, and R. T. D. Sousa, ‘‘Trust-based security for the OLSR routing protocol,’’ Comput. Commun., vol. 36, nos. 10–11, pp. 1159–1171, Jun. 2013.
[11] A. B. C. Douss, R. Abassi, and S. G. E. Fatmi, ‘‘A trust management based security mechanism against collusion attacks in a MANET environment,’’ in Proc. 9th Int. Conf. Availability, Rel. Secur., Sep. 2014, pp. 325–332.
[12] B. Wang and X. Chen, ‘‘Opportunistic routing algorithm based on trust model for ad hoc network,’’ J. Commun., vol. 34, no. 9, pp. 92–104, 2013.
[13] A. Nabou, M. D. Laanaoui, and M. Ouzzif, ‘‘New MPR computation for securing OLSR routing protocol against single black hole attack,’’ Wireless Pers. Commun., vol. 115, pp. 1–20, Nov. 2020.
[14] N. C. Singh and A. Sharma, ‘‘Resilience of mobile ad hoc networks to security attacks and optimization of routing process,’’ Mater. Today, Proc., 2020. [Online]. Available: https://www.sciencedirect.com/ science/article/pii/S2214785320373478, doi: 10.1016/j.matpr.2020.09.622.
[15] M. Faraji-Biregani and R. Fotohi, ‘‘Secure communication between UAVs using a method based on smart agents in unmanned aerial vehicles,’’ J. Supercomput., vol. 76, pp. 1–28, Nov. 2020.
[16] R.-R. Yin, N. Zhao, and Y.-H. Xu, ‘‘An selective forwarding attack con- sidered routing protocol for scale-free network,’’ in Proc. 12th Int. Symp. Commun. Syst., Netw. Digit. Signal Process. (CSNDSP), Jul. 2020, pp. 1–6.
[17] K. Rajesh Kumar, Balaji.M, Deepak.S, Harsha.C, Karthikeyan.K **“ Train Collusion Avoidance System With Braking Units”,** International Research Journal of Engineering and Technology (IRJET), ISSN 2395-0056, Vol 8,Special Issue 5, PP 37-40, May 2021. **https://www.irjet.net/archives/V8/i5/IRJET-V8I511.pdf** Impact Factor value: 7.529
[18] R.Velumani & M.Vijayakumar 2019, “IoT based Prudent Automatic Falls Detection for Elders by Analyzing Carrier State Information (CSI) Employing WiFi Devices” Wireless Personal Communications, pp. 1-16, DOI:10.1007/s11277-019-06168-6.
[19] K. Rajesh kumar1, K. Mohan Raj, A. S. Murugan3, K. Naveen, K. Prakash, **“Enhanced Brailee Display Use of OCR and SOLENOID to Improve Test to Brailee Conversion”,** International Research Journal of Engineering and Technology (IRJET), ISSN 2395-0056, Vol 8, Special Issue 5 ,PP 113-115, May 2021. **https://www.irjet.net/archives/V8/i5/IRJET-V8I531.pdf**
[20] Velumani, R & Vijayakumar, M 2018 “Prudent Automatic Falls Detection by Analyzing Carrier State Information (CSI) Signal Using Wi-Fi Devices” Journal of Testing and Evaluation(ASTM International), Vol.47, no.4,pp.2947-2963.

ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology
An ISO 3297: 2007 Certified Organization *Volume 11, Special Issue 1, April 2022*
9th National Conference on Frontiers in Communication and Signal Processing Systems (NCFCSPS '22)
28 th -29 th April 2022
Organized by
Department of ECE, Adhiyamaan College of Engineering, Hosur, Tamilnadu, India

[21] Rajesh Kumar.K, Shilpa.R, Swathi Priya. P, Uma Mageshwari.K, Yuvadharshini.JB, **"An Auto Pilot System by Extracting Images on Live Video Frame 25 fps and Robust Driving Efficiency with Speed Control",** International Research Journal of Engineering and Technology (IRJET), ISSN 2395-0056, Vol 8,Special Issue 5, PP 133-136, May 2021. https://www.irjet.net/archives/V8/i5/IRJET-V8I537.pdf

BIOGRAPHY

MR.K.RAJESH KUMAR
ELECTRONICS AND COMMUNICATION ENGINEERING DEPARTMENT,
ADHIYAMAAN COLLEGE OF ENGINEERING,
ANNA UNIVERSITY

S.SUNIL KUMAR
ELECTRONICS AND COMMUNICATION ENGINEERING DEPARTMENT,
ADHIYAMAAN COLLEGE OF ENGINEERING

G.THIRUMAL
ELECTRONICS AND COMMUNICATION ENGINEERING DEPARTMENT,
ADHIYAMAAN COLLEGE OF ENGINEERING

YUVAN R.M
ELECTRONICS AND COMMUNICATION ENGINEERING DEPARTMENT,
ADHIYAMAAN COLLEGE OF ENGINEERING,

S.BALACHANDARAN
ELECTRONICS AND COMMUNICATION ENGINEERING DEPARTMENT,
ADHIYAMAAN COLLEGE OF ENGINEERING,

INNO SPACE
SJIF Scientific Journal Impact Factor
Impact Factor: 8.118

doi cross ref

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details