Advances in Science, Technology and Engineering Systems Journal Vol. 7, No. 2, 25-31 (2022)

www.astesj.com

ASTESJ

ISSN: 2415-6698

Taxonomy of Security Techniques for Routing Protocols in Mobile Ad-hoc Networks

Kartit Zaid*,[1,2], Diouri Ouafaa[2]

[1]*Mohammed V University in Rabat, Presidency of Mohammed V University, Innovation Center, Rabat, 10102, Morocco*

[2]*Mohammed V University in Rabat, Computer Science Department, Mohammadia School of Engineering, Rabat, 10102, Morocco*

ARTICLE INFO

Article history:

Received: 25 November, 2021
Accepted: 26 January, 2022
Online: 11 March, 2022

Keywords:
MANETs
Security Routing
Authenticity
Trust

ABSTRACT

The Nodes equipped with wireless technology cooperate in an autonomous and instantaneous way to form a mobile ad hoc network. It turns out that several factors make this type of network vulnerable to various security threats. Considering the sensitivity of user data routed through nodes, routing security should be a priority in mobile ad hoc networks (MANET). Techniques and schemes have been proposed to secure the basic routing protocols in order to guarantee the availability of information routing services between network nodes. The majority of the solutions presented in the literature belong to two categories, namely those that use cryptographic techniques and those that use trust schemes. Given the characteristics of MANET networks, we need approaches that guarantee a level of honesty of the nodes to prevent possible routing attacks from malicious nodes. This study presents the security extensions of the basic routing protocols AODV, DSR and DSDV.A first part is devoted to extensions based on cryptography and a second part introduces extensions using trusted systems. Then we discussed and analyzed them while drawing up a comparative table to measure the effectiveness of the mechanisms used as well as the limits and strengths of each proposed extensions. In this study, we conclude that a new trust model that combines an access strategy with lightweight techniques must be developed to ensure honest node behavior can be a key to securing the routing protocol in MANET.

1. Introduction

Mobile Ad hoc Network is becoming an interesting research field as it offers great flexibility and a fast and fluent dynamic implementation. Indeed, mobile ad hoc network MANET (Fig. 1) is an autonomous system consisting of a collection of nodes that are interested in communicating via a wireless link. In MANET, the node is self-configured without the need for any central administration and can communicate directly with neighbors. But to communicate with out-of-range nodes, it requires the cooperation of other intermediate nodes which act as routers to establish reliable and optimal route [1].

The absence of a communication administration makes the deployment of mobile ad hoc networks easier. But the reliability of routing information exchanged between nodes when establishing routes and maintaining them presents a challenge because these networks have characteristics that make them more vulnerable to attack from malicious node. This last node cannot respect the routing protocol rules by disturbing the routing process by inserting false information in the routing messages, modifying their content's or simply not cooperating by deleting them. Indeed, several studies in the literature have shown that the nodes are exposed to several threats security of routing protocol and in [2] they has established a taxonomy of attacks detected in the MANET. Although cryptographic techniques have been widely used in routing to protect routing information, such an approach may not be practical for real MANETs due to heavy computational loads and the lack of ability to detect attacking nodes [3].

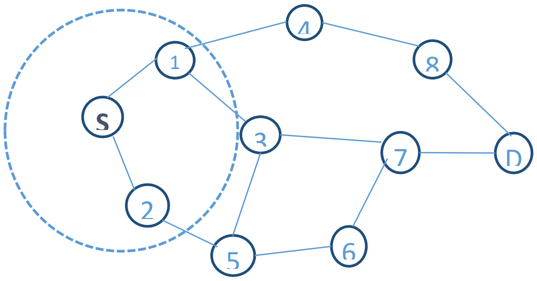

Figure 1: A Mobile Ad hoc Network

[*] Corresponding Author: Kartit Zaid, Email: zaid.kartit@um5.ac.ma

https://dx.doi.org/10.25046/aj070203

Nodes continually join and leave networks. It turns out that taking into consideration the notion of "trust" in ad hoc networks is very useful in a highly dynamic environment where nodes must depend on each other to accomplish their common goals. A trust system allows each node of the network to observe and predict the behavior of its neighbors in an efficient manner, with the objective of selecting honestly cooperating nodes.

Therefore, trust-based routing has been seen as an effective measure to manage security threats caused by malicious nodes through detection and isolation of untrusted nodes in the network [3]. Only, to create a reliable communication environment, a distributed trust system that supports network access control and honest cooperation, according to specific routing protocols is needed to help nodes achieve their mission in the mobile network ad hoc.

This paper is organized as follows, section 2 introduces security routing in MANETs, section 3 describe and discuss the different techniques deployed by researchers to solve partially the problem of routing security, then section 4 present the security analyses of extensions studied. Then we conclude our study and discussion in Section 5.

2. Routing protocol and security in MANET

For an ad hoc mobile network, a routing protocol is considered the first part to ensure self-training of such a network. In the literature the researchers did not take into consideration the security aspect that made MANETs networks very vulnerable to attacks. A necessary first action that such a protocol must ensure is to ensure that each node cooperates in an honest way.

Any attack on the routing process disrupts communications between network nodes and can go up to and disrupt the entire network. A second action can be summarized in that it takes into consideration the constraints posed by the scarcity of resources available to nodes such as residual energy, storage capacity.

To provide security services the previous studies in [1][4] have outlined several solutions classified in two categories namely prevention mechanism or detection and reaction mechanism [5][1]. The first one involves encryption techniques particularly to ensure the authenticity and integrity of messages. The latter is used for detecting malicious behavior of dishonest nodes.

Therefore, we can say that a Routing Protocol in MANETs networks can be considered as a communication model whose components and the role of each of them must be specified.

3. Techniques for secure routing in MANET

This paper is an extension of previously published conference paper originally presented in Networking, Information Systems & Security conference NISS19 [1]. This section presented some relevant security extensions of the AODV, DSDV and DSR. We have classified them into two categories, the first approach based on cryptography systems and the second based on trusted schemes.

3.1. Cryptographic techniques

Cryptography systems are widely used in the security of communication networks. It is in the continuity of use of such systems that researchers have applied them to secure routing protocols in ad hoc networks. In the following we present various cryptography solutions used to secure routing protocol in MANETs. In our previous work published at ACM [1], we has compared and analyzed some extensions of DSR, DSDV and AODV protocols based on cryptographic techniques. In addition to these extensions, we present others in this paper that we consider relevant to solve the problem of routing security in MANET networks. Indeed a common point of these models is that they focus on the importance of identity and decentralized aspect that must be taken into consideration.

Concerning the DSR protocol we cite two extensions which used two different techniques. In the first extension [6] the authors proposed a SecDSR security extension of DSR protocol based on Ariadne protocol which relies on symmetric cryptography that is able to authenticate the source who initiated route discovery process. In fact this extension integrated the message authentication code (MAC) mechanism to provide a point-to-point authentication of routing messages between two nodes in mobile ad hoc network. In the second extension [7] the authors integrated in DSR protocol the sequential aggregate ID-based signatures (IBSAS). In fact, during the route discovery phase to validate the routing information, each intermediate node participates in the calculation of the IBSAS signature conveyed in SRREQ. This allows the destination node to verify the signature in the SRREQ using the IDs of intermediate nodes received by IBSAS verification. ISDSR reduce memory size and compute overhead. Therefore ISDSR helps eliminate dishonest nodes in a route. ISDSR can ensure the validity of route information when a route is constructed.

As for the DSDV protocol, in order to ensure the authentication and the integrity of the messages, extensions have incorporated mechanisms based on asymmetric cryptography. In [8] the authors presented dAN DSDV an extension of the DSDV protocol using a message authentication code based on an asymmetric cryptographic approach to establish an optimal secure path. The certification and validation of the RREQ message are performed at each node when moving from one node to another using a paired shared secret key mechanism in the routing path. The proposed method ensures both the authentication and the integrity of the message with packet loss and delay minimized, throughput and packet delivery rate maximized. To allow mutual authentication between two network nodes in [9] the authors proposed a mutual Hash-MAC-DSDV scheme by making a modification of the DSDV protocol. This scheme adopts a structure of a cluster network where the CH nodes facilitate the registration of nodes in a local channel at first and broadcast it via nodes called base stations to register it in a second called public channel. This process allows the network node to update their routing table to be able authenticate each node requesting communication. Indeed, before transmission, a unidirectional authentication process is performed to verify the legitimacy of each node by matching Hash MAC with their table of MAC addresses. This scheme has demonstrated its effectiveness in terms of attack, detection metrics, power consumption and communication cost.

Attack prevention is considered an effective way to provide a level of security for the AODV protocol. Node identification and key management have been used to strengthen its security. Indeed, in [10] the authors integrated the HiMAC mechanism to secure the distribution of data in AODV. Based on trust and message authentication the HiMAC's technique prevent an intruder from capturing routing information, which makes it easier for him to carry out attacks by generating a diversion of the route thus causing a black hole attack. This prevents intruders from altering or modifying the number of hops by using signature and encryption of messages at each intermediate node. This approach is based on identity-based cryptography and message authentication code (MAC). In fact, each intermediate node will add its MAC and its timestamp, in addition to its ID to the list of message identifiers. In this scheme, each node shares its public key with other "trusted" nodes only. HiMAC require an efficient public key management system or the key size must be optimal to reduce encryption and decryption times and the size of the data messages is not very large. In [11]the authors proposed a new SAODV protocol scheme by introducing a short digital signature scheme for authentication. The use of the short digital signature aims to gain the same level of security but with more efficiency and less computation. In this scheme another signature assignment mechanism is to use a trusted third party to share secret digital signatures with each node in the network and establish secure communications between two nodes by signature-based authentication. In this scheme the hash function was used to authenticate the hop count.

3.2. Technical Trust

The designers of routing protocols for ad-hoc networks have considered that the intermediate nodes cooperate in the respect of the specificities of said protocol by expressing an honest behavior. This supposed trust allows malicious nodes to easily generate attacks on the routing process. Indeed, malicious nodes can deliberately behave in such a way as to disrupt the content of the packets and consequently disrupt the routing process. Several security mechanisms have been proposed to protect routing information against attacks by malicious nodes, to establish a reliable and efficient communication path. Many approaches and proposals have been proposed to address various trusted ad hoc secure routing schemes.

A malicious node is considered a primary source of attack for basic protocols such as AODV.to eliminate this type of attack in [12], [1] the authors presented a trust mechanism named TDS-AODV. This mechanism has been modified AODV routing protocol to implement the trust model of TSDRP [13] to prevent malicious actions like Blackhole and DoS attacks by calculating the trust value for their neighbor. In this AODV extension, a node makes a routing decision based on the trust values of its neighbor nodes. Finally, two routes are built: the main route with the highest route trust value in the candidate routes and the backup route. This mechanism has proven its ability to eliminate malicious nodes during the construction of the route. This extended protocol above highlights efforts to introduce and improve reliability in mobile ad hoc networks using trusted systems.

To ensure the existence of links to route messages in the MANET in [14] the authors have proposed a Trusted Recover AODV (TR-AODV) model based on the identity authentication scheme and the existing TAODV trust model. Their model requires a node to join the network to be authenticated in two cases where it is the first time or if it has a trust level less than the threshold. This model encourages nodes already registered by an identity to join the network by resetting their trust level to the threshold value. This will guarantee the availability of routing service and push the nodes to cooperate and behave normally according to the system of trust. If his cooperation is verified, he improves his trust value. Otherwise, it will go to the blacklist. This technique has the impact of good management of malicious nodes by giving them a second chance to participate effectively in the network. Consequently, packet loss is reduced and transmission delay is improved.

In another scheme the addition of data structure seems necessary to route the messages between nodes in order to distribute trust in the network. Indeed in [15] the authors proposed ESTA protocol based on AODV by introducing two new data structures LINK_TABLE and LINK_INFO. Each node serves as a LINK_TABLE mechanism to first record the information contained in the RREQ requests received and in a second to generate a LINK_INFO control message once it is part of a path. The latter makes it possible to update its availability and that of the next node in the LINK_TABLE table of neighboring nodes. This protocol works without a certification authority; however, it combines a system of trust with asymmetric cryptography to ensure the integrity and authentication of control messages. To satisfy the authenticity of the messages, it encrypts the node identity and the timestamp value by the private key of the source node. Another data structure called SOURCEINFO is used to store the level of the trust value vis-à-vis the network nodes. This value is communicated by another control message SEND DELIVERY_INFO. All of this impacts communication delay due to the overhead introduced by these control packets and data structures. Another disadvantage is that the trust system is limited to direct observations. Indeed, in the absence of interaction between two nodes or sharing of trust with other network nodes, a malicious node being out of range can respond to its RREQ message leaving the source node unable to make a good decision. It is desirable to consider indirect observations, especially since they have added control messages and data structures that can help ensure good management of the trust.

The selection of the path among others is always based on the number of hops to reach the destination. But in [16] the authors have proposed the ReTE-AODV based protocol which uses the level value of trust as a path selection parameter to guarantee the honest commitment of the nodes which will transmit the data packets. The proposed algorithm routes the messages not by the shortest route, but by selecting a reliable trustworthy route that consumes little power and has a level of trust for sending the packets. To do this the trust value is obtained from direct and indirect trust. The calculation of the trust value is based on the direct and indirect trust and to refine this value they adopted the Bayesian method. The same thought to change the paradigm of the choice of the route in [17] the authors have proposed a multi-factor routing strategy named EOSR protocol. This extension of the AODV protocol adopts a distributed trust model that helps to detect and isolate malicious attacks. In their solution the choice of the route is based on three metrics that is residual energy, trust level and number of hop count. The behavior of the node is used to calculate the level trust. In order to improve the accuracy of the trust value they required to obtain the indirect trust from the common adjacent nodes. However, to filter out false notes from malicious nodes, any indirect trust collected by an adjacent node must have excluded false notes that exceed the Thdeviation threshold. Trust and energy information is added in routing messages without increasing communication traffic. As for path selection, they defined a new metric called total path cost taking into account the confidence value, the residual energy and the number of hops count. One of the major advantages of this extension is that it takes into account the dynamic change of the network topology.

In order to demonstrate a level of trust, several measures must be taken into consideration. This is why in [18] the authors proposed a system called SCOTRES, integrated into DSR, based on trust to secure the routing of the mobile ad hoc network. This system advances the intelligence of network node by applying five new measures. The energy metric to measure the level of cooperation expected from each node. The dynamic topology metric anticipate the change position of node. The channel quality metric gives an idea of the reliability of the node. The reputation metric assesses the cooperation of each participant in a specific network operation, detecting attacks, while the trust measure estimates overall compliance, protection against combinatorial attacks. In another view in [19] the authors have proposed the DSR Enhanced Trust (TEDSR) based on trust to establish stable and reliable routes. It includes the payment systems in a trust-based routing protocol. The goal is to establish the stable route to reduce the liability of route breaks. The enhanced DSR protocol establishes the best path that can meet the requirements of the source node including energy, trust level and route length, and incorporated this information's into routing messages (RREQ, RREP).

Finally in [20] the authors presentend a model based on the Blockchain structure (BATM) to ensure authentication and trust in sensor networks. The Blockchain is used to facilitate the management of public keys, digital signature and peer information. Consequently, each node of the network has the possibility of validating the information on all the other nodes of the network. The BATM module includes a trust model called Human-based Knowledge-Based Trust (HKT), which is based on human behavior to maintain a reputation level for each node. It uses the payloads contained in the Blockchain to measure the behavior of each node. In this way, it ensures that a node cannot deceive others by falsifying data or impersonating someone else. Thus, it assesses trust, without the need for a trust center.

4. Security analysis, discussion, and comparative study

The reliability of the information diffused through the control messages in the different phases of routing is the basis for a secure routing protocol solution. In fact, an ad hoc network is a network that necessitates a degree of cooperative trustworthiness where each node must respect the specifications of the routing protocol.

For the first category based on cryptography, the various solutions deployed above are dedicated to the authenticity of the nodes and the integrity of the routing messages. Given the characteristics of the MANETs networks, the proposed solutions go toward techniques that combine symmetric cryptography systems and hash functions. On the other hand, asymmetric cryptography systems secure efficiently but are not easily adaptable for this type of network. Several mechanisms are used to prevent active attacks that affect the update of messages and their authenticity as digital signature, message authentication code (MAC), one-way hash functions, hashed MAC (HMAC), or a combination of these techniques [1].To secure validity of the route information when a route is constructed several solutions have been developed such as:

In dAN EFFICIENT DSDV the destinations can verify the integrity of the message using a hash chain calculated at the time of broadcasting of the RREQ. As for the authentication it is ensured by including the identity of each participating node in the hash code. Therefore, this technique provides both authenticity and integrity of routing packets. We consider this mechanism efficient since it proves the honest of the intermediate nodes to establish the secure and guard the path establishing. In SecDSR, the authors used the TESLA hash chain to calculate the code MAC as well as a hash accumulation including the identity of each intermediate node to prevent corruption of path information's. ISDSR is based on digital signature to trust the information communicated by a node. In effect, indeed to participate in the creation of the route it is necessary to have an identifier and a secret key and this to prove a first level of trust towards others. Only the drawback of this approach is the fact that it requires the existence of a server for managing identifiers and keys for each node. In addition, it requires each node to reserve a memory space to store the keys. The Hach-MAC-DSDV scheme adopts a network zoning to facilitate the management of the network nodes. Each zone is administered by a CH zone manager and a local chain which records the hash of the MAC address of the nodes registered in the network. A public chain is established between the different CH. this allows the creation of a decentralized pseudo-administration to ensure the authentication of the participating nodes by creating a secure authentication key for each node. A major vulnerability of this model is that it allows each node to register with its MAC address, which is not enough to prevent a malicious node from subsequently carrying out an attack once it has access to the network. HiMAC is one of the first techniques which is based in the first place on cryptographic tools based on the identity of the nodes and the MAC code and in a second on the confidence of the participating nodes in the dissemination of messages in the network. HiMAC can be efficient with a light PKI and with a powerful identification system.

Although cryptographic techniques have been widely used to protect routing information based on checking the authenticity and integrity, such an approach is not sufficient to secure routing in MANET networks. We observe in the whole of the preceding diagram that the identity of the nodes plays a primordial role in ensuring the security of the routing protocols in an ad hoc network. With this in mind, other extensions belonging to a second category based on trust have emerged by introducing the notion of trust to help nodes to observe and predict the behavior of neighboring nodes efficiently [3]. Trust-based systems extend the level of node cooperation that goes beyond simple verification. Indeed, in the ad hoc network, each node measures a trust level of the nodes before entering into interaction with them. Each extension is based on a scheme to assess the confidence of the nodes. Direct observations, recommendations from others, and other factors can change a node's trust level [21] .Most of the extensions studied in this paper consider that path selection should take into consideration the trust level of and not just the number of hops. Such a trust level is not limited to the behavior of the nodes, but it's extended to other factors such as residual energy, the quality of the available channel, and the dynamic aspect of the topology [22].

The TR-AODV protocol considers that the availability of a cooperating node is necessary, so these authors have adopted the restoration of the reputation of nodes via a node authentication mechanism before accessing the network. We believe that this action is very necessary to eliminate dishonest nodes from sharing the network and to get others to cooperate honestly. The EOSR protocol is a multi-factor routing protocol based on a distributed trust model that takes into account the dynamic aspect of the network. As for the SCOTRES protocol, it integrates the intelligence of the nodes of the network by applying five new measures to assess the level of confidence of the nodes. It exhibits the best power and load balancing behavior, provides the highest level of security, and handles certain types of attacks that other systems cannot counter. Another very important measure is introduced in the ESTA protocol which does not require a certification authority. BATM provides an easy way to manage trust in decentralized Blockchain-based networks and takes more parameters into account in assessing trust and reputation.

In summary, in the first part of our table below we notice that the cryptography-based extensions are unable to preventing all security threats. We also concluded [1] that these protocols should not consider all network nodes as trusted. Therefore, the way they build the roads is to be reviewed. Another point that makes routing security more complex is the dynamically changing network topology, which makes the paths breakable and unstable. In addition, we can say that security must be ensured for the entire system because a single weak point can give the attacker the ability to access the system and perform malicious tasks. In second part of our table we consign that each extensions based trusted system provides a technique to reduce the drawbacks of cryptography. And others that allow routing protocols to be adapted to the characteristics of Ad Hoc networks, such as the notion of autonomous and distributed management, the measurement of the quality of interaction between network nodes.

Indeed, we have identified three essential points to take into consideration in our future work to secure a routing protocol in MANET's networks. At first, we will develop a new distributed trust system in which trust will not only depend on authentication, we will define a metric to measure the behavior of the nodes, each node must show its honesty in the forwarding process of messages. Then, an efficient method to calculate the index of the reputation of the nodes seems to us necessary. We will use this index to define the level of trust. As a second step, we also propose a revision of the RREQ broadcast approach in which we will limit access to routing information to nodes with a certain level of trust. In fact, the new nodes will have a low level of trust. By cooperating with honest behavior, their level of trust becomes great. We recall that in ad hoc networks the nodes are considered trustworthy when they arrive. In our approach, we will reverse this principle by applying the method described above [1].

5. Conclusion

This paper reviewed a taxonomy extension security grouped by technics used in various researches to secure the routing protocols. Different approaches based on cryptography and / or on trusted systems are proposed to prevent routing attacks in MANET networks. These approaches try to provide an optimal path composed of secure node by implementing different mechanisms in existing routing protocols. We have seen the limit of cryptography-based solutions either in terms of adapting to the resource constraints that this type of network suffers or in responding to security objectives. As for trust-based protocols, most extensions consider that the path selection should take into consideration the level of trust and not just the number of hops in the path selection. Such a trust level is not limited to the behavior of the nodes but also to other factors such as residual energy, the [1] quality of the available channel and the dynamic aspect of the topology. But we have observed other limitations which are more precisely linked to the identification system and the characteristics of Ad hoc networks. Finally, this study will help us in our future work to introduce other technologies based on the hardware properties of nodes to facilitate the management of the identities of the nodes that we consider the security gate of these protocols.

Conflict of Interest

The authors declare no conflict of interest.

Table 1: Comparison of secure extensions routing protocols in Mobile Ad Hoc network

Extension	Attacks	Parameters and Mechanisms	Advantages	Disadvantages
dAN-DSDV	Malicious	HMAC,ID	Packet drop excluded Delay time decreased with increasing the security level	energy consumption overhead
SecDSR	Malicious	Tesla, hash chain, ID	More security than DSR	increases routing overheads congestion in the network
ISDSR	Malicious	IBSAS, aggregate signatures	decrease the memory size and the computational overhead better latency	management server required
Hash-MAC-DSDV	Sybil, Dos Eavesdropping	lightweight Hash-MAC clustering local and public chain ,one-way-hash authentication	Legitimacy of node guaranteed Better attack detection rate minimal resource consumption	difficult to implement

HiMAC-AODV	Tampering data, replay attack	MAC, Digital Signature , trust schemes	higher success ratio, less hop count, smaller packet queue size secure routing dynamically	high overhead high processing overhead
SAODV	Blackhole Grey hole	Short digital signature, Hash function	reducing the computational power	signature distribution center required
TR-AODV	Replay Selfish	Authentication and Reputation Restoring and Increasing Chances for Normal Communication (Availability)	Data loss rate reduced , Incentive for node cooperation Better network Improved network access ,Delay reduced Communication quality	Authentication and reputation restoration scheme load to consider
ESTA	Blackhole	Trust level, Identity encryption control packages add	not use CA or additional processing at intermediate	Limited to direct observation, Consumes more resources additional delay
ReTE-AODV	Malicious	Trust level energy consumption	Good level of security with a better packet delivery ratio and reduced average end-to-end latency.	Consumes more energy, routing packet overload
EOSR	Malicious	Residual energy, CCP full path cost , Distributed trust model	Best performance in terms of delivery rate, throughput with average energy consumption. Support the dynamic aspect	End-to-end delay is not included in the performance metric
TEDSR	Blackhole	three levels of trust Payment report	Path securing by validation of intermediate nodes by the source node identify fraudulent nodes accurately and quickly without false accusations or missed detections	Transfer-based trust level calculation method is not sufficient to measure the behavior of nodes. Not tested in the presence of malicious nodes.
SCOTRES	flooding Blackhole, link-spoofing	Uses five metrics: residual energy, channel quality, topology, reputation and trust levels	Best behavior in terms of energy and load balancing, provides the highest level of security and handles certain types of attacks that other systems cannot counter.	Consumes more resources Additional traffic overload
BATM	DOS	Blockchain PKI Trust level	Simple way to manage trust in decentralized Blockchain-based networks. takes more parameters into account when assessing trust and reputation levels	First block creation Lack of performance measurement Storage space required for the Blockchain

References

[1] Z. Kartit, O. Diouri, “Security extension for routing protocols in Ad hoc mobile networks: A comparative study,”ACM International Conference Proceeding Series, Part F1481, 2019, doi:10.1145/3320326.3320403.

[2] N.A. Noureldien, “A novel taxonomy of MANET attacks,” Proceedings of 2015 International Conference on Electrical and Information Technologies, ICEIT 2015, 109–113, 2015, doi:10.1109/EITech.2015.7162947.

[3] M.S. Pathan, N. Zhu, J. He, Z.A. Zardari, M.Q. Memon, M.I. Hussain, “An efficient trust-based scheme for secure and quality of service routing in MANETs,” Future Internet, 10(2), 2018, doi:10.3390/fi10020016.

[4] A.K. Abdelaziz, M. Nafaa, G. Salim, “Survey of routing attacks and countermeasures in mobile ad hoc networks,” Proceedings - UKSim 15th International Conference on Computer Modelling and Simulation, UKSim 2013, 693–698, 2013, doi:10.1109/UKSim.2013.48.

[5] K. Vijayakumar, K. Somasundaram, “Study on reliable and secure routing protocols on Manet,” Indian Journal of Science and Technology, 9(14), 2016, doi:10.17485/ijst/2016/v9i14/84433.

[6] M.K. Hameed, F.J.Abd-Razak,“A Secure dynamic source routing protocol for mobile ad hoc networks,”, journal of kerbala university **15**,issue 4, 32-41-2017

[7] K. Muranaka, N. Yanai, S. Okamura, T. Fujiwra, “ISDSR: Secure DSR with ID-based sequential aggregate signature,” ICETE 2016 - Proceedings of the 13th International Joint Conference on e-Business and Telecommunications, 4(Icete), 376–387, 2016, doi:10.5220/0006001003760387.

[8] Ch. Anusha, E. Laxmi Lydia, T. Pavani, Ch. Usha Kumari, M. Ilayaraja Kanagaraj Narayanasamy, “ dAN efficient dsdv routing in mobile networks through symmetric cryptographic method,” , Journal of critical reviews ISSN- 2394-5125 VOL 7, ISSUE 10, 2020. doi:10.31838/jcr.10.31.

[9] M. Adil, M.A. Jan, S. Mastorakis, H. Song, M.M. Jadoon, S. Abbas, A. Farouk, “Hash-MAC-DSDV: Mutual Authentication for Intelligent IoT-Based Cyber-Physical Systems,” IEEE Internet of Things Journal, 4662(c), 1–11, 2021, doi:10.1109/JIOT.2021.3083731.

[10] K. Mershad, A. Hamie, M. Hamze, “HiMAC: Hierarchical Message Authentication Code for Secure Data Dissemination in Mobile Ad Hoc Networks,” International Journal of Communications, Network and System Sciences, 10(12), 299–326, 2017, doi:10.4236/ijcns.2017.1012018.

[11] M.T. Abbas, M.A. Khan, A. Khaliq, N.A. Saqib, J. Ahmad, S. Rehman, “Secure AODV Protocol for Mobile Networks Using Short Digital Signatures,” Proceedings - 2017 International Conference on Computational Science and Computational Intelligence, CSCI 2017, 645–650, 2018, doi:10.1109/CSCI.2017.111.

[12] R. Feng, S. Che, X. Wang, N. Yu, “A credible routing based on a novel trust mechanism in Ad Hoc networks,” International Journal of Distributed Sensor Networks, 2013, 2013, doi:10.1155/2013/652051.

[13] A. Aggarwal, S. Gandhi, N. Chaubey, K.A. Jani, “Trust based secure on demand routing protocol (TSDRP) for MANETs,” International Conference on Advanced Computing and Communication Technologies, ACCT, 432–

438, 2014, doi:10.1109/ACCT.2014.95.

[14] J. Liu, S. Huan, "Trust recovery model of Ad Hoc network based on identity authentication scheme," AIP Conference Proceedings, 1839(May), 2017, doi:10.1063/1.4982566.

[15] D. Singh, A. Singh, "Enhanced secure trusted AODV (ESTA) protocol to mitigate blackhole attack in mobile Ad hoc networks," Future Internet, **7**(3), 342–362, 2015, doi:10.3390/fi7030342.

[16] Priya Sethuraman, N. Kannan, "Refined trust energy-ad hoc on demand distance vector (ReTE-AODV) routing algorithm for secured routing in MANET," Wireless Networks, **23**(7), 2227–2237, 2017, doi:10.1007/s11276-016-1284-1.

[17] T. Yang, X. Xiangyang, L. Peng, L. Tonghui, P. Leina, "A secure routing of wireless sensor networks based on trust evaluation model," Procedia Computer Science, **131**, 1156–1163, 2018, doi:10.1016/j.procs.2018.04.289.

[18] G. Hatzivasilis, I. Papaefstathiou, C. Manifavas, "SCOTRES: Secure Routing for IoT and CPS," IEEE Internet of Things Journal, **4**(6), 2129–2141, 2017, doi:10.1109/JIOT.2017.2752801.

[19] R. Pricilla, T.R. Vedhavathy, "TRUSTED ENHANCED DSR FOR IMPROVING PAYMENT SCHEME IN MWN," (December), 2–6, 2014.

[20] A. Moinet, B. Darties, J.-L. Baril, "Blockchain based trust & authentication for decentralized sensor networks," (June), 2017.

[21] Z. Hao, Y. Li, "An adaptive load-aware routing algorithm for multi-interface wireless mesh networks," Wireless Networks, **21**(2), 557–564, 2015, doi:10.1007/s11276-014-0804-0.

[22] K. Kundu, C. Chowdhury, S. Neogy, S. Chattopadhyay, "Trust aware directed diffusion scheme for wireless sensor networks," Proceedings - 4th International Conference on Emerging Applications of Information Technology, EAIT 2014, 385–391, 2014, doi:10.1109/EAIT.2014.68.