A NOVEL NATURE INSPIRED SECURE AND TRUSTWORTHY ROUTING PROTOCOL FOR MANET

[1*]Moresh Mukhedkar, [2]Uttam D. Kolekar, [3]Vaishali S. Jadhav, [4]Pallavi Sapkale

[1,3,4]Assistant Professor, [2]Principal

[1]E&TC Department, D. Y. Patil University, Ambi, Pune, Maharashtra, India

[2]E&TC Department, A. P. Shah Institute of Technology, Thane, Maharashtra, India

[3,4]E&TC Department, Ramrao Adik Institute of Technology, D. Y. Patil Deemed to be University, Nerul, Navi Mumbai, India

(*moresh.mukhedkar@gmail.com)

Abstract: Mobile ad-hoc networks (MANET's) are the wireless networks becomes popular due to its self-organized nature i.e. they don't have any fixed or centralized infrastructures, like traditional wired telecommunication networks those are highly depends on towers as well as sophisticated base station. Hence due to this reason they are utilized in many kinds of applications. Routing is one of the important aspects present in MANET, it is responsible for transfer of data packets from source node to the destination node via shortest route, hence for the said purpose nature inspired algorithms are effectively used just like Dolphin Echolocation and Glowworm Swarm optimization. While transfer of packets through many nodes, packet data security is much needed. Advanced Encryption Standard algorithms used for providing encryption to the data available in the packets. Hence by integration of nature inspired algorithms and security algorithm, a novel routing protocol is developed having prominent results for the fixed size of MANET.

Key Words - MANET, AES, Dolphin, Routing Protocol, Security.

1. INTRODUCTION

Now a day, ad-hoc networks are becoming increasingly popular and have been put into practice in many kinds of applications. Ad-hoc networks are self-organized wireless networks without fixed or centralized infrastructures. Nodes in ad-hoc networks act as both clients and routers [7]. A mobile ad hoc network (MANET) or wireless ad hoc network (WANET) is a decentralized type of wireless network in that set of electronics device that uses wireless data connections between wireless network nodes which dynamically connect and transfer information. Wireless nodes can be personal computers (desktops/laptops) with wireless LAN cards, Personal Digital Assistants (PDA), or other types of wireless or mobile communication devices [8]. Further MANET networking is a method by which homes, telecommunications networks and business installations avoid the costly process of introducing cables into a building, or as a connection between various equipment locations. Wireless telecommunications networks are generally implemented and administered using radio communication [9, 19]. This implementation takes place at the physical level (layer) of the OSI model network structure. Examples of wireless networks include networks of Cell phone, wireless local area networks (WLANs), wireless sensor networks, satellite communication networks, and terrestrial microwave networks. The MANET does not rely on a pre-existing infrastructure, such as routers in wired networks or access points in managed (infrastructure) wireless networks. And these MANETs can also be the temporary and provisional to deal with a particular wireless network related problem. Figure 1. Illustrates what MANET is.

In such network instead, each node participates in routing by forwarding data for other nodes, so the determination of which nodes forward data is made dynamically on the basis of network connectivity and the routing algorithm in use.

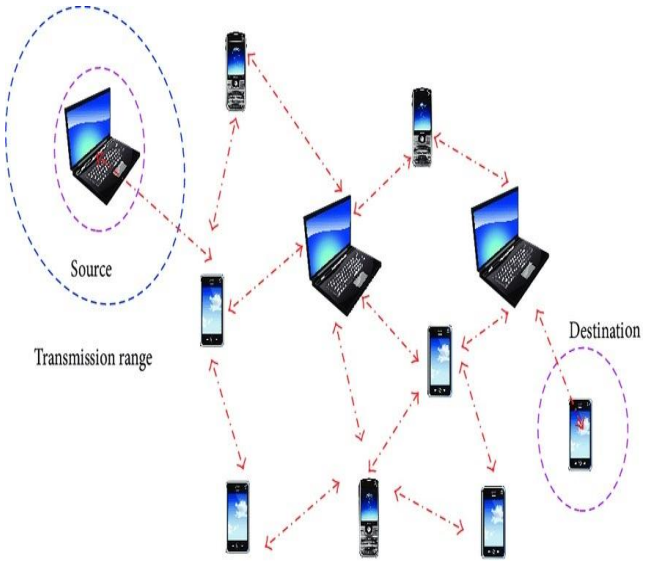

Fig.1 MANET Overview (figure from Angle and Context Free Grammar Based Precarious Node Detection and Secure Data Transmission in MANETs)

Wireless networks lack the complexities of infrastructure setup and administration, enabling devices to create and join networks "on the fly" – anywhere, anytime. In general, a wireless node can be any computing equipment that employs the air as the transmission medium. As shown, the wireless node may be physically attached to a person, a vehicle, or an airplane, to enable wireless communication among them. In MANET, a wireless node can be the source, the destination, or an intermediate node of data transmission. When a

wireless node plays the role of intermediate node, it serves as a router that can receive and forward data packets to its neighbor closer to the destination node. Due to the nature of MANET, wireless nodes tend to keep moving rather than stay still [11, 12]. Therefore the network topology changes from time to time.

Hence we can easily describe MANET as a continuously self-configuring, infrastructure-less network of mobile devices connected wirelessly. Each device in a MANET is free to move independently in any direction, and will therefore change its links to other devices frequently. Each must forward traffic unrelated to its own use, and therefore be a router. The primary challenge in building a MANET is equipping each device to continuously maintain the information required to properly route traffic. Such networks may operate by themselves or may be connected to the larger Internet. They may contain one or multiple and different transceivers between nodes [13]. This results in a highly dynamic, autonomous topology [14]. MANETs are a kind of WANET that usually has a routable networking environment on top of a Link Layer ad hoc network. MANETs consist of a peer-to-peer, self-forming, self-healing network. MANETs circa 2000–2015 typically communicate at radio frequencies (30 MHz – 5 GHz).

1.1 Nature-Inspired Routing Protocol

Nature has inspired many researchers in many ways and thus is a rich source of inspiration. Nowadays, most new algorithms are nature-inspired, because they have been developed by drawing inspiration from nature. Even with the emphasis on the source of inspiration, we can still have different levels of classifications, depending on how details and how many sub sources we will wish to use. For simplicity, we will use the highest level sources such as biology, physics or chemistry. In the most generic term, the main source of inspiration is Nature. Therefore, almost all new algorithms can be referred to as nature-inspired. By far the majority of nature-inspired algorithms are based on some successful characteristics of biological system. Therefore, the largest fractions of nature-inspired algorithms are biology-inspired, or bio-inspired for short [15, 16]. Among bio-inspired algorithms, a special class of algorithms has been developed by drawing inspiration from swarm intelligence. Therefore, some of the bio inspired algorithms can be called swarm-intelligence (SI) based.

1.2. Security aware routing in MANET

There are two phases for performing communication in the MANET namely, route discovery and data transmission. These two phases are affected by the different types of attacks. Initially, the malevolent nodes interrupt the route discovery phase by the following activities; distributing the forged control traffic, imitating the destination, responds to hard or contaminated routing information. In this manner, the attackers block the dissemination of the legal route control traffic and persuade the benign node's topological knowledge [17]. The malevolent nodes interrupt the data transmission phase by the following activities; introducing the forged data packets, illegal redirecting, and dropping the data traffic [18]. Hence, there is a need of secure routing protocols for securing both phases in communication since the nodes do not guarantee the secure delivery of the data because the malevolent nodes are located on the transmission path.

2. Literature Survey

The development of real time secure routing algorithms for Mobile ad hoc Network (MANET) is carried and optimized trust based routing is the major and important challenge. Routing is defined as the process of choosing paths for transmitting the data packets in a network. Along with routing data security and Quality of Service (QoS) awareness is also important factors. There are number of routing mechanisms have been proposed for MANET. In this chapter, the various routing techniques along with, trust mechanism, data encryption for secure communication in MANET is discussed.

The author Jaspal Kumar et al. [1] developed Secure route discovery in AODV in presence of black hole attack. This algorithm having advantages like is simple to implement and no additional overhead is required on resource constrained devices. The limitations of this are increasing delay in data packet delivery.

Gautam M. Borkar and A. R. Mahajan [2] in their paper A secure and trust based on-demand multipath routing scheme for self-organized mobile ad-hoc networks. Discussed about advantages like Enhance the quality of routing and had find the best path by the optimization algorithm. Their work having limitations like their proposed protocol is only allowed to accept an alternate route with smaller hop count in accordance with the trust requirement.

Jarupula Rajeshwar and Gugulotu Narsimha [3] in their paper Secure way routing protocol for mobile ad hoc network. They have advantages like Secure the routing mechanism from both the internal and the external attacks. The effects of mobility have high impact on the performance of mobile ad-hoc network are the limitations of their work.

Amit Kumar *et al.* in their work [4] A novel next hop selection based secure routing for wireless ad hoc sensor networks Resilience against the attackers who shares the numerous messages. Increased route length is the limitation of this method.

Shushan Zhao *et al.* [5] worked on A key management and secure routing integrated framework for Mobile Ad-hoc Networks.

More secure due to the use of node-specific broadcast key instead of only 1 group broadcast key. The proposed framework does not provide the monitoring.

Jian Shen *et al.* [6] developed and published work on organized topology based routing protocol in incompletely predictable ad-hoc networks. Provide better performance in node utilization frequency is the advantage of their work. And limitation of their method is that it does not suitable for larger network.

Shuaishuai Tan *et al.* [7] in their paper A Trust Management System for Securing Data Plane of Ad-Hoc Networks. Found the advantages like their Trust management system is effective and efficient in protecting the data plane of ad-hoc networks. The limitation of this algorithm is that it requires that the number of malicious and victim nodes should be less than the number of normal ones.

3. Proposed MANET routing protocol using Encrypted Trust based Dolphin Glowworm Optimization

The proposed Encrypted Trust Based Secure Routing Protocol using Dolphin Glowworm Optimization Algorithm that offers security in MANET routing, using AES-128 and DGO algorithm. Encrypted Trust Based Secure Routing Protocol using Dolphin Glowworm Optimization Algorithm is comprised of three steps, such as k-path discovery, optimal path selection, and data communication. This involves routing message broadcast through RREQ and RREP phase, wherein AES-128, shared code and shared key provides a secure data transmission by encrypting the message. Based on the distance and the trust level of the nodes, k-paths are discovered. For the optimal selection of routes, an optimization algorithm, DGO, is developed that selects the routes based on a suitable fitness function [14]. Then, the data will be transmitted through the path selected after the encryption of the message using AES-128, for the security. The proposed Encrypted Trust Based Secure Routing Protocol using Dolphin Glowworm Optimization Algorithm used for routing is illustrated using the block diagram shown in figure 2.

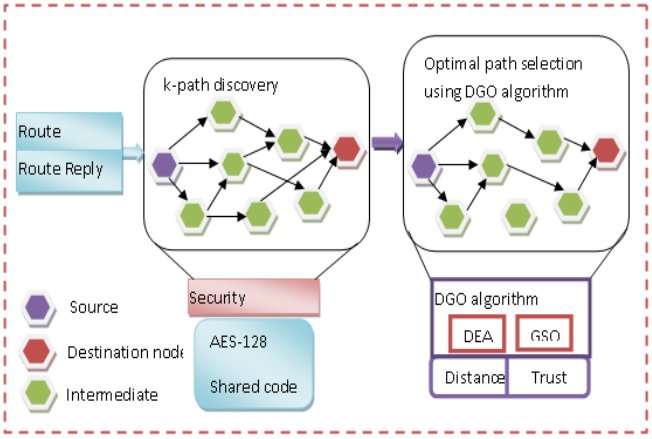

Fig. 2. Block diagram of the proposed Encrypted Trust Based Secure Routing Protocol using Dolphin Glowworm Optimization Algorithm for MANET routing

4. ENCRYPTED TRUST BASED ROUTE DISCOVERY

This section presents the Novel protocol that offers security in MANET routing, using AES-128 and DGO algorithm. Novel protocol is comprised of three steps, such as k-path discovery, optimal path selection, and data communication. This involves routing message broadcast through RREQ and RREP phase, wherein AES-128, shared code and shared key provides a secure data transmission by encrypting the message. Based on the distance and the trust level of the nodes, k-paths are discovered. For the optimal selection of routes, an optimization algorithm, DGO, is developed that selects the routes based on a suitable fitness function. Then, the data will be transmitted through the path selected after the encryption of the message using AES-128, for the security.

4.1. ROUTE REQUEST PHASE

The node that desires to begin the route discovery process for the communication becomes the source node, and it transmits an RREQ message to its neighboring nodes, as given in the following format,

$$M_{RQ} = \{f_{RQ}, AES(S_C), D_{ID}, TTL\} \quad (1)$$

where, f_{RQ} is the message flag, which is set 1, implying RREQ message, D_{ID} is the destination ID, S_C is the shared code and TTL represents the time to live field. To confirm that the node is not an attacker, the node that receives the encrypted shared code evaluates S_C^* as,

$$S_C^* = Decr(AES(S_C)) \quad (2)$$

where, $Decr(.)$ represents the decryption process. Computing S_C^* as in equation (13), the shared code is obtained using the shared key S_K by comparing if $S_C^* = S_C$. The node checks whether it is the intended receiver by comparing its ID, denoted as X_{ID}, with D_{ID}. If a match is found, then the node is identified as the destination node and it does not transmit the message further to other nodes. In the other case, the node continues the transmission by retransmitting the message request to its neighbors. TTL field defines the time interval at which the transmission is to be completed. E-TDGO protocol rejects the data packets that reach the node once TTL is expired as the time reaches beyond the maximum limit, denoted as $\max\_time$.

4. 2 ROUTE REPLY PHASE

Each node that receives M_{RQ} undergoes an RREP phase, where a reply message is sent to the node that transmitted the message. The RREP message format is given by,

$$M_{RP} = \{f_{RP}, AES(S_C \| X_{ID} \| S_K)\} \quad (3)$$

where, f_{RP} is the message flag that implies RREP message and $f_{RP} = 1$, X_{ID} is the ID of any node X that can be either intermediate node, denoted here as n_b, or destination node n_D. The shared code is encrypted in a node using AES-128 after concatenating the code with its ID and S_K; and it is transmitted along with f_{RP} to the source node. On receiving the reply message, the source node decrypts the shared code and the ID of the node that transmitted M_{RQ} from $AES(S_C \| X_{ID} \| S_K)$ by validating the shared code as,

$$S_C^* = Decr(AES(S_C \| X_{ID} \| S_K)) \quad (4)$$

Thus, confirms whether the node that forwarded the message packet is malicious or normal by checking whether $S_C^* = S_C$.

4.3 SECURED DATA COMMUNICATION PROCESS USING THE PROPOSED PROTOCOL

This section presents the communication process carried out using Encrypted Trust Based Secure Routing Protocol using Dolphin Glowworm Optimization Algorithm. Here, the data considered for the communication is the speech

data, which is transmitted as message packets. The data communication process is illustrated by a diagram shown in figure 2, where the communication takes place through a source-destination pair.

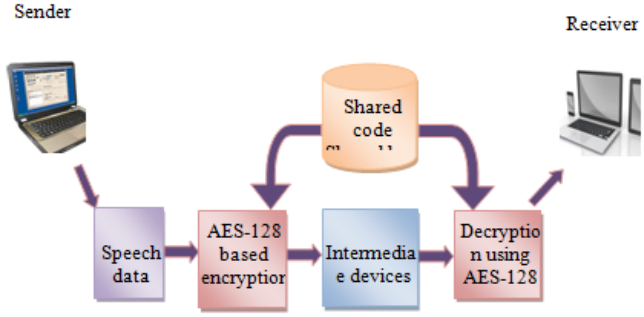

Fig. 3. Speech data communication using proposed protocol

5. Results And Discussion

Table 1, table 2, and table 3 shows the analysis based on the performance metrics, in the presence and absence of the attacks. In the absence of the attacks, the proposed method acquired the average throughput, delay, packet drop, and detection rate. The proposed method acquired better performance when compared with the existing methods. Table 2 shows the comparative analysis in the presence of the black-hole attack. The proposed method acquired the average throughput, delay, packet drop, and detection rate. Table 3 shows the comparative analysis in the presence of a Sybil attack. The proposed method acquired the average throughput, delay, packet drop, and detection rate. It is proved from table 1, table 2, and table 3 that the proposed method acquired a better performance with higher throughput, minimal delay, minimal packet drop, and maximal detection rate.

Table 1. Performance comparison of network based on 75 nodes without an attack

Methods	Evaluation Measures			
	Average Throughput	Delay	Packet drop	Detection rate
AOMDV-SAPTV	0.3739	0.0114	0.6444	0.9733
TBS-OLSR	0.3864	0.0121	0.6222	0.9778
AES-DGO	0.2111	0.0121	0.6822	0.9763
Proposed Protocol	0.5141	0.0114	0.4667	0.9896

Table 2. Performance comparison of network based on 75 nodes with a black-hole attack

Methods	Evaluation Measures			
	Average Throughput	Delay	Packet drop	Detection ra
AOMDV-SAPTV	0.2612	0.0116	0.6911	0.9733
TBS-OLSR	0.2564	0.0119	0.6378	0.9719
AES-DGO	0.2979	0.0123	0.6556	0.9719
Proposed Protocol	0.5871	0.0116	0.4422	0.9881

Table 3. Performance comparison of network based on 75 nodes with Sybil attack

Methods	Evaluation Measures			
	Average Throughput	Delay	Packet drop	Detection ra
AOMDV-SAPTV	0.2635	0.0117	0.6644	0.9585
TBS-OLSR	0.2759	0.0119	0.6553	0.9585
AES-DGO	0.4543	0.0121	0.5805	0.9585
E-TDGO	0.5035	0.0117	0.4399	0.9926

6. Conclusion

The development of a Novel nature inspired Secure and Trustworthy routing protocol for MANET is performed, the features like secure transmission using AES and optimized routing performed using integration of Dolphin echolocation and Glowworm swarm protocol. The comparative analysis of proposed protocol and other existing routing protocols such as AOMDV-SAPTV, TBS-OLSR and AES-DGO is done. The proposed protocols are having better results when compared with the existing protocol. The performance parameters used for comparison are Throughput, delay, packet drop and detection rate. Total numbers of nodes consider are 75. The main findings for proposed protocol for 75 nodes with black hole attack are, Average Throughput - 0.5871, Delay - 0.0116, Packet drop - 0.4422, and Detection rate is 0.9881.

References

[1] Jaspal Kumar, M. Kulkarni ,Daya Gupta, S. Indu, “Secure route discovery in AODV in presence of blackhole attack”, CSI Transactions on ICT, Vol. 3, No. 2, pp. 91–98, December 2015.

[2] Gautam M. Borkar, A. R. Mahajan, “A secure and trust based on-demand multipath routing scheme for self-organized mobile ad-hoc networks”, Wireless Networks, .

[3] Jarupula Rajeshwar, et.al, “Secure way routing protocol for mobile ad hoc network”, Wireless Networks, pp. 1–10, 2015.

[4] Amit Kumar, Vijay Kumar, Kamal Kumar, “A novel next hop selection based secure routing for wireless ad hoc sensor networks”, CSI Transactions on ICT, pp. 1–7, 2016.

[5] Shushan Zhao, Robert Kent, Akshai Aggarwal, “A key management and secure routing integrated framework for Mobile Ad-hoc Networks”, Ad Hoc Networks, Vol. 11, No.3, pp. 1046–1061, May 2013.

[6] Jian Shen, Chen Wang, Anxi Wang, Xingming Sun, Sangman Moh, Patrick C.K. Hung, “Organized topology based routing protocol in incompletely predictable ad-hoc networks”, Computer Communications, Vol. 99, , pp.107–118, February 2017.

[7] Shuaishuai Tan, Xiaoping Li, Qingkuan Dong, “A Trust Management System for Securing Data Plane of Ad-Hoc Networks” IEEE Transactions on Vehicular Technology, Vol. 65, No.9, pp. 7579-7592, September 2016.

[8] T. Dutta, “Medical data compression and transmission in wireless ad hoc net- works”, IEEE Sensors Journal, Vol. 15, No. 2, pp.778-786, February 2015.

[9] T. Shu, M. Krunz, “Privacy-preserving and truthful detection of packet dropping attacks in wireless ad hoc networks”, IEEE Transactions on Mobile Computing, Vol. 14, No. 4, pp.813-828, April 1 2015.

[10] Deng, H, et.al. “Routing security in wireless ad hoc networks”, IEEE Comm. Magazine, Vol.40, No.10, pp.70-75, Oct 2002.

[11] Jing, Q, Vasilakos A. V, Wan J, Lu J, Qiu, D, “Security of the internet of things: Perspectives and challenges”, Wireless Networks, Vol. 20, No. 8, pp. 2481–2501, November 2014.

[12] Wei L., Zhu H., Cao Z., Jia W, Vasilakos, A. V, “Seccloud: Bridging secure storage and computation in cloud”, In proceedings of IEEE 30th International Conf. distributed computing systems workshops (ICDCSW), pp. 52–61, 2010.

[13] Boukerche A, Turgut B, Aydin N, Ahmad MZ, Boloni L, Turgut D, "Routing protocols in ad hoc networks: a survey", Computer Networks, Vol. 55, No. 13, pp. 3032–3080, 15 September 2011.

[14] Moresh M. Mukhedkar, Dr. Uttam D. Kolekar, "Trust-Based Secure Routing in Mobile Ad Hoc Network Using Hybrid Optimization Algorithm", The Computer Journal, Oxford University Press, Vol. 62, issue 10, pp. 1528-1545, Oct 2019.

[15] Lacuesta, R., Lloret, J., Garcia, M., Pen˜alver, L, "A secure protocol for spontaneous wireless ad hoc networks creation", IEEE Transactions on Parallel and Distributed Systems, Vol. 24, No. 4, pp. 629–641, 2013.

[16] Shelke S. K. (2020, Low Power High Frequency Implementation of Image Filtering using Improved Median Filtering, International Journal of Advanced Science and Technology, Vol. 29, No. 4s, (March 2020), pp. 1833-1843.

[17] Satyanarayana R et.al. "Performance Enhancement of Rectangular Microstrip Antenna With Different Substrate Materials." Int. Journal of Innovative Technology and Exploring Engineering (IJITEE), Vol. 9, Issue-2S, Dec. 2019.

[18] Vaishali Satish Jadhav, Uttam D. Kolekar, "Fuzzy-based decisive approach for call admission control in the LTE networks", Evolutionary Intelligence, Volume 13, Issue 3, September 2020.