International Journal of Advanced Computer Technology
ISSN: 2319-7900 www.ijact.org Volume 12, Issue 2, April 2023

An Optimised and Efficient Routing Protocol Application for IoV: A Review

Mayank Soni, Jitendra Singh
Electronic Communication Department
Babulal Tarabai Institute of Research & Technology, Sagar (M.P), India
sonimayank347@gmail.com, jksingh.indi@gmail.com

Abstract: Mobile ad hoc network (MANET) is a wireless network without a centralised administrator, where each node acts as a router forwarding data packets to other nodes. The study compares the performance of three routing protocols (AODV, OLSR, and DSDV) using the NS2 simulator under various mobility models. The proposed work introduces a modified protocol, MAODV, which combines the features of AODV protocols to optimise energy consumption, minimise transmissions, and find an optimum path for data transmission. The proposed method is compared with the standard AODV protocol. It shows better average throughput and packet delivery ratio results in a vehicular ad hoc network (VANET) scenario.

Keywords: MANET, Wireless, Vehicular Ad Hoc Network, Routing Protocol, AODV Protocol, Clusters

I. Introduction

A mobile ad-hoc network (MANET) is a collection of mobile nodes that operate without a fixed infrastructure, dynamically changing their geographic locations. These networks have dynamic topologies and limited resources, making them susceptible to network partitions. MANETs are commonly used in military or police networks, business operations, and emergency response operations in natural disasters. However, the open operating environment and multi-hop routing in MANETs make them vulnerable to attacks from malicious nodes, such as black-hole and grey-hole attacks. In this dissertation, we propose using detection as a defense technique against black hole attacks. For detection, we use a profile-based detection technique to gather information about the offender node, such as the node type, number of attack packets, attack time, and so on. We then prevent black hole attacks using a neighbour trust-based technique to secure the mobile ad-hoc network communication. Our proposal aims to provide secure and reliable communication and simulate the network behaviour in attack and prevention cases using Network Simulator-2. Additionally, we evaluate the performance of the network based on network parameters such as turnout, packet delivery ratio, throughput, routing load, and so on. By using a trustworthy node-based approach, we expect higher successful electronic communication rates to be achieved.

1.1 Security Aspect in MANET

In order to ensure the security of Ad-hoc On-demand Distance Vector (AODV), it is essential to have a clear understanding of the security features and mechanisms involved. Applying security to AODV involves a combination of processes, procedures, and systems to achieve confidentiality, authentication, integrity, availability, access control, and non-repudiation [4]. As Mobile Ad-hoc Networks (MANETs) employ an open medium, all nodes within the communication range can access data. Hence, the following measures need to be taken into account to ensure the security of AODV:

1. Confidentiality must be maintained to prevent unauthorised nodes from accessing data.
2. Authentication is essential to verify the identity of the nodes, which helps prevent unauthorised access to confidential information and resources, as well as interference with the operations of other nodes.
3. Integrity is critical to prevent malicious nodes from altering and resending data (known as a replay attack, such as a wormhole attack).

4. Non-repudiation ensures that a node cannot deny sending a message once it has been sent [5].

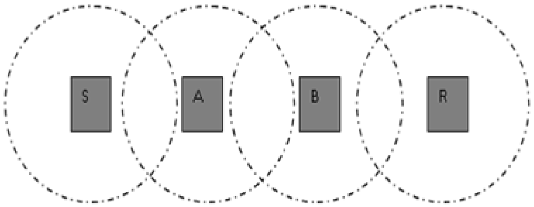

Figure1 Example of MANET

The vulnerabilities of operational systems and higher-layer applications of user programs, such as databases, browsers, or client-server applications, are often not considered a security issue for unexpected networks [6]. General attack types can threaten the routing layer of the MANET, including the physical, MAC, and network layers, which are critical functions of ad-hoc wireless networks for routing mechanisms, familiarising the packets during a route discovery process. Other vulnerabilities, such as application security, network security, and information security, have been studied in several works but are not explained here in detail. Attacks on the ad-hoc wireless network at the networking layer typically serve two purposes: not forwarding packets or adding and changing certain routing messages parameters, such as sequence numbers and destination addresses. These are explained in the following sections. Using one of the key mechanisms, such as cryptography or authentication [7], or both, in a network is a preventive approach that can be used against attackers. However, while these mechanisms protect the network against external attacks, malicious insiders possessing one essential key can also threaten security. For example, in a battlefield scenario where MANETs are employed, even if the keys are protected by tamper-proof hardware used in the vehicles within the network, it is challenging to guarantee that these vehicles will exhibit the same behaviour if the enemy captures them.

On the other hand, a node may unintentionally behave as if it is malfunctioning. For example, a node with a failing battery that cannot perform network operations may be perceived as an attack. Another malicious behaviour of nodes is stinginess. Self-seeking nodes conserve their resources, such as battery power, by not participating in network operations. Therefore, failing and self-seeking nodes also impact network performance as they do not properly process network packets, such as in routing mechanisms. We must ensure everything is operating correctly within the network to support overall security and identify how an insider can attack the Mobile Ad hoc Network (MANET). MANETs should be protected with an intrusion detection system that can detect the possible actions of attackers and produce a solution against these attacks. In order to defend against passive attacks, conventional approaches such as digital signatures, encryption, authentication, and access control (i.e., whether a node has appropriate access rights to access the network) should be considered. To defend against active attacks, intrusion detection systems and cooperation enforcement mechanisms (reducing the selfish behaviour of a node) are useful. Encryption and authentication rely on asymmetric and symmetric cryptography [7]. Hash functions and digital signatures are useful for achieving data integrity and authentication.

1.2 Need for Security in Ad Hoc Networks

Although mobile ad-hoc networks are widely used, they still have some weaknesses that require the need for security to address these issues [1, 6]. An attacker may take advantage of these weaknesses to gain information about the network processes and launch an attack on the network. The following are some vulnerabilities that exist in ad-hoc networks:

1. Mobility: Every node in a mobile ad-hoc network is movable and can join or leave a network at any time without informing any node. This allows an attacker to enter the network and even participate in its operations easily.
2. Open Wireless Medium: All communication between nodes occurs through airwaves rather than wired connections. An attacker can easily access this medium to intercept communication or launch attacks.
3. Resource Constraints: Each node in a mobile ad-hoc network has limited resources such as battery, processing power, and bandwidth. An attacker can consume these resources without permission, rendering them unusable.
4. Dynamic Network Topology: The network's topology changes frequently as nodes move around, and the packets from source to destination may take different paths. An

attacker can position themselves in any path to intercept or modify communication.

5. Scalability: Mobile ad-hoc networks can contain many nodes, and the number is not fixed. An attacker can take advantage of this parameter as there is no limitation on the number of nodes in the network.
6. Reliability: Wireless communication is limited to a range of 100 meters, which imposes a constraint on nodes to be in range for establishing communication. Due to this limited range, data errors are also generated. An attacker must be in that node's range to attack a specific node.

1.3 Routing

Primarily three routing protocols are used in networks: proactive, reactive, and hybrid. In proactive routing protocols, each node maintains one or more tables representing the complete topology of the network. These tables are updated regularly to maintain up-to-date routing information from every node to each other node. In order to keep up-to-date routing information, topology information must be exchanged between the nodes regularly, which results in relatively high overhead on the network. The advantage is that routes are always available on demand.

In contrast, reactive routing protocols do not initiate a route discovery process until a route is needed. This results in higher latency than with proactive protocols but lower overhead. Hybrid protocols maintain the topology information within their zone and the information regarding neighbouring zones, meaning proactive behaviour within a zone and reactive behaviour among zones. Thus, a route to every destination within a zone is established instantaneously, while a route discovery and maintenance procedure is required for destinations in other zones.

II. Literature Survey

The previous work provides information about the security scheme in MANET. Some of the schemes are mentioned below: -

Kiran Afzal et. al. [2]. IoV is the latest application of VANET and is the alliance of the Internet and IoT. With the rapid progress in technology, people are searching for a traffic environment where they would have maximum collaboration with their surroundings, which comprise other vehicles. Finding a traffic environment with less traffic congestion, minimum chances of a vehicular collision, minimum communication delay, fewer communication errors, and a greater message delivery ratio is necessary. For this purpose, a vehicular ad hoc network (VANET) was devised where vehicles communicated in an infrastructure-less environment. In VANET, vehicles communicate ad hoc and communicate with each other to deliver messages, for infotainment purposes or to warn other vehicles about emergency scenarios. Unmanned aerial vehicle- (UAV-) assisted VANET is one of the emerging fields nowadays. For VANET's routing efficiency, several routing protocols are being used, like optimised link state routing (OLSR) protocol, ad hoc on-demand distance vector (AODV) routing protocol, and destination-sequenced distance vector (DSDV) protocol. In order to meet the need of the upcoming era of artificial intelligence, researchers are working to improve the route optimisation problems in VANETs by employing UAVs. The proposed system is based on a model of VANET involving interaction with aerial nodes (UAVs) for efficient data delivery and better performance. Comparisons of traditional routing protocols with UAV-based protocols have been made in vehicle-to-vehicle (V2V) communication. Later on, vehicle communication via aerial nodes was studied for the same purpose. These results have been generated through various simulations. After performing extensive simulations by varying different parameters over grid sizes of 300 ×1500 m to 300 × 6000 m, it is evident that although the traditional DSDV routing protocol performs 14% better than drone-assisted destination-sequenced distance vector (DA-DSDV) when we have the number of sinks equal to 25, the performance of drone-assisted optimised link state routing (DA-OLSR) protocol is 0.5% better than that of traditional OLSR. In contrast, drone-assisted ad hoc on-demand distance vector (DA-AODV) performs 22% better than traditional AODV. Moreover, suppose we increase the number of sinks up to 50. In that case, it can be clearly seen that the DA-AODV outperforms the rest of the routing protocols by up to 60% (traditional or drone-assisted). In addition, for parameters like MAC/PHY overhead and packet delivery ratio, the performance of our proposed drone-assisted variants of protocols is also better than that of the traditional routing protocols. These results show that our proposed strategy performs better than the traditional VANET protocols and plays an important role in minimising the MAC/PHY and enhancing the average throughput and packet delivery ratio. Hussain et al. [9] proposed a Denial of Service (DoS) attack in AODV and feature extraction for style detection engine for Intrusion Detection Systems (IDS) in Mobile Ad hoc Networks (MANETs). The work involves applying a DoS attack in the network and collecting evidence to design the intrusion detection engine for MANET IDS. Feature extraction and rule induction techniques are employed to determine the accuracy of the detection engine using Support Vector Machine (SVM). The detection engine exhibits high True Positive and negligible False Positive rates. True Positive generated by the detection engine is reported quickly, and Friend lists generated by Lids are sent to the Gids module for further investigation. The Global Detection Engine can generate a friend list that aligns with the trust level, which is also used for routing and cluster head selection in scalable ad-hoc networks. The features extracted for routing and MANET traffic generation parameters are used for various routing protocols. The detection engine employs the Support Vector Machine, which is lightweight and considered the best among the supervised learning algorithms. The prediction accuracy generated by the SVM for input options and different values of C and λ is satisfactory for the given training and testing datasets. Jing-Wei Huang et al. [10] proposed Multi-Path Trust-Based Secure AOMDV Routing in Unpredictable Networks. This work proposes a trust-based multi-path AOMDV routing scheme combined with soft encoding called T-AOMDV. This approach consists of three steps: (1) Message encoding - at the source node, the message is segmented into three parts, and these parts are encrypted using XOR operations, (2) Message routing - the message parts are routed individually through different trust-based multiple paths using a novel node-disjoint AOMDV protocol, and (3) Message decoding - the destination node decrypts the message parts to recover the original message. Shreenath et al. [11] planned Countermeasures against Multicast Attacks on Enhanced-On Demand Multicast Routing Protocol in MANETs. This work concentrates on raising the Secure Enhanced-On Demand Multicast Routing Protocol (EODMRP) to safeguard it against flooding and black-hole attacks. The planned mechanism for flooding attacks works even once the identity of the malicious nodes is unknown and doesn't use any extra network bandwidth. The performance of a little multicast cluster can degrade seriously below these kinds of attacks, even if the answer is obtainable. The planned algorithm protects against region attacks in MANET. Sujatha et al. [12] proposed a genetic algorithm-based IDS for painters to analyse the vulnerability of AODV to attacks, specifically the most common network layer hazard, region attack. The proposed system is a specification-based Intrusion Detection System (IDS) that uses a genetic algorithm approach. The system analyses the behaviours of each node and provides details about the attack. Genetic algorithm control (GAC) is a set of various rules based on the important features of AODV, such as Request Forwarding Rate and Reply Receive Rate. Konate et al. [13] proposed an attack analysis in mobile ad hoc networks (MANETs): modelling and simulation. In this paper, the authors present a work devoted to reviewing attacks and countermeasures in MANETs, briefly introducing what MANETs are and network security. They present a survey of various attacks in MANETs related to failed routing protocols, as well as the different tools employed by these attacks and the mechanisms utilised by secured routing protocols to counter them. In this paper, they also define the concept of Denial of Service (DoS) attacks and its various types. The authors provide several examples of DoS attacks that are common in MANETs, their operational methods, and the mechanisms and protocols that can be used to counter these attacks. Gandhewar et al. [14] proposed a mechanism for detecting and preventing sinkhole attacks on the AODV protocol in mobile ad hoc networks. This work primarily focuses on the sinkhole problem and its consequences and presents a mechanism for detecting and preventing it in the context of the AODV protocol. A sinkhole is one of the severe types of attacks that attempts to attract most of the network traffic towards it and degrade the network's performance. AODV has been mainly analysed under blockhole, wormhole, and flooding attacks, but it also needs to be analysed under other types of attacks. The performance of AODV with no sinkhole attack, vulnerable, and when applying our mechanism in the form of simulation result obtained for sure variation of nodes in the network by considering performance metrics as output, PDR, end-to-end delay, and packet loss. The proposed work by PK Singh et al. [15] aims to provide an efficient solution for preventing the black hole problem in the AODV routing protocol in MANET. The black hole problem is a type of region attack that involves a malicious node advertising a false shortest path to the destination node, leading to disruption of communication. The proposed approach uses the promiscuous mode to detect the black hole node and disseminates this information to all other nodes in the network.

III. Expect Outcome

The primary issue in the field of MANET is security due to the presence of unexpected threats. A new research study highlights numerous obstacles in this field. Mobile ad hoc network (MANET) has emerged as a new end-to-end solution for providing connectivity anywhere, at any time. However, MANETs are more vulnerable due to their dynamic and open nature, which leads to security being the primary concern. The study's primary goal is to observe several network performance measures, such as recognising packet delivery ratio, enhancing routing performance, monitoring constantly harmful symptoms, and lowering overhead using good local route repair maintenance. The routing (overhead) load specifies how many routing packets are needed for route discovery and maintenance. The lower the number of routing packets, the higher the performance. Throughput represents the total number of bits forwarded to higher tiers per second and is measured in bits per second (bps). The packet Delivery Ratio is the ratio of incoming data packets to the number of data packets received. A higher percentage ratio depends on better data reception in a dynamic network. The study aims to minimise routing (overhead), maximise throughput, and achieve a good PDR.

Conclusion

This review article addresses the requirement for continuously monitoring security and privacy challenges and solutions in IoV. The benefits of a specific routing protocol in a mobile ad-hoc network depend on aspects such as network size, load, and mobility needs. IoV primarily involved information exchange between roadside units, humans, and automobiles and was developed to manage vehicles and avoid accidents and road hazards. It refers to vehicle-to-vehicle communication across a network and uses traditional routing protocols such as DSDV, OLSR, and AODV. This paper proposes a modified AODV protocol that extends network life and finds the best path from source to destination to develop an efficient routing system. The proposed solution's performance was evaluated by comparing energy usage, PDR, and delay time with the existing AODV protocol, and the new method was found to outperform the existing method. The efficiency characteristics of the proposed system are expected to be higher on average, including improved throughput, packet delivery ratio, reduced MAC/PHY overhead focus, reduced end-to-end delay, and a low packet drop ratio. The proposed approach was implemented using the NS2 simulator.

References

[1]. J. Wang, X. Xiao, and P. Lu, "A survey of vehicular ad hoc network routing protocols," Journal of Electrical and Electronic Engineering, vol. 7, no. 2, pp. 46–50, 2019.

[2]. Afzal, K., Tariq, R., Aadil, F., Iqbal, Z., Ali, N., & Sajid, M., "An optimised and efficient routing protocol application for IoV. Mathematical Problems in Engineering, 2021.

[3]. Oscar F. Gonzalez, God Win Ansa, Michael Howarth and George Pavlou. "Detection and Accusation of Packet Forwarding Misbehavior in Mobile Ad-Hoc Networks", Journal of Internet Engineering, Vol.- 2, no.1, 2008.

[4]. Sunil Taneja and Ashwani KushA Survey of Routing Protocols in Mobile Ad Hoc Networks International Journal of Innovation, Management and Technology, Vol. 1, No. 3, August 2010.

[5]. Sudhir Agrawal, Sanjeev Jain, Sanjeev Sharma, "A Survey of Routing Attacks and Security Measures in Mobile Ad-Hoc Networks", Journal of Computing, Volume 3, Issue 1, January 2011.

[6]. K. P. Manikandan, Dr R. Satya Prasad, Dr K. Rajasekhara Rao, "A Survey on Attacks and Defense Metrics of Routing Mechanism in Mobile Ad hoc Networks, (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 2, No.3, March 2011.

[7]. S. Yi and R. Kravets, "Composite Key Management for Ad Hoc Networks". Proceedings of the 1st Annual International Conference on Mobile and Ubiquitous Systems: Networking and Services (MobiQuitous'04), pp. 52-61, 2004.

[8]. K. Sivakumar, Dr G. Selvaraj, "Overview of Various Attacks in MANET and Countermeasures for Attacks", International Journal of Computer Science and Management Research Vol 2 Issue 1 January 2013.

[9]. Husain, Shahnawaz, Gupta S.C., Chand Mukesh "Denial of Service Attack in AODV & Friend Features Extraction to Design Detection Engine for Intrusion Detection System in Mobile Adhoc Network", International Conference on Computer & Communication Technology (ICCCT-2011), pp. 292- 297, 2011.

[10]. Jing-Wei Huang, Isaac Woungang, Han-Chieh Chao, Mohammad S. Obaidat, Ting-Yun Chi, Sanjay K. Dharanidhar "Multi-Path Trust-Based Secure AOMDV Routing in Ad Hoc Networks", Proceedings of IEEE Global Telecommunications Conference (GLOBECOM 2011), pp. 1-5, 2011.

[11]. Dr N. Sreenath, A. Amuthan, & P. Selvigirija "Countermeasures against Multicast Attacks on Enhanced-On Demand Multicast Routing Protocol in MANETs", International Conference on Computer Communication and Informatics (ICCCI -2012), pp. 1-7, 2012.

[12]. K. S. Sujatha, Vydeki Dharmar, R. S. Bhuvaneswaran "Design of Genetic Algorithm based IDS for MANET", International Conference on Recent Trends in Information Technology (ICRTIT), pp. 28-33, 2012.

[13]. Dr Karim KONATE, GAYE Abdourahime "Attacks Analysis in mobile ad hoc networks: Modeling and Simulation", 2011 Second International Conference on Intelligent Systems, Modelling and Simulation, pp. 367 – 372, 2011.

[14]. Gandhewar, N., Patel, R. "Detection and Prevention of Sinkhole Attack on AODV Protocol in Mobile Adhoc Network", Fourth International Conference on Computational Intelligence and Communication Networks (CICN), pp. 714 – 718, 2012.

[15]. P. K Singh, G. Sharma, "An Efficient Prevention of Black Hole Problem in AODV Routing Protocol in MANET", IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), pp. 902 – 906, 2012.