TẠP CHÍ KHOA HỌC ĐẠI HỌC HẠ LONG
Scientific Journal of Ha Long University
http://uhl.edu.vn/

ANALYSIS OF ATTACK METHODS AND SECURITY SOLUTIONS FOR AODV ROUTING PROTOCOL IN WIRELESS AD HOC NETWORKS

Ngô Hải Anh[1*]

[1]*Viện Công nghệ thông tin, Viện Hàn lâm Khoa học và Công nghệ Việt Nam*

** Email: ngohaianh@ioit.ac.vn*

Ngày nhận bài: 28/04/2023 Ngày nhận bài sửa sau phản biện: 01/06/2023 Ngày chấp nhận đăng: 20/06/2023

ABSTRACT

The Ad-hoc On-Demand Distance Vector (AODV) routing protocol, designed for unstructured or ad hoc wireless networks, is suitable for mobile links or network nodes capable of processing power and does not need to be high. However, AODV will be preserved if we pay attention to the security solutions used in the design of this protocol. This paper analyzes several vulnerabilities, especially discusses AODV attacks based on routing messages. We will demonstrate how to authenticate, ensure the integrity of routing messages, and use specification-based intrusion detection to detect attacks against the AODV protocol.

Keywords: *AODV, digital signature, hash chains, intrusion detection, MANET, network monitor, SAODV, specification-based detection.*

PHÂN TÍCH MỘT SỐ PHƯƠNG THỨC TẤN CÔNG VÀ GIẢI PHÁP BẢO MẬT CHO GIAO THỨC ĐỊNH TUYẾN AODV TRONG MẠNG KHÔNG DÂY AD HOC

ABSTRACT

Giao thức định tuyến Ad-hoc On-Demand Distance Vector (AODV) được thiết kế cho các mạng không dây phi cấu trúc hoặc Ad hoc, phù hợp với các liên kết di động hoặc các nút mạng có khả năng xử lý và không cần hiệu năng cao. Tuy nhiên, nếu chúng ta chú ý đến các giải pháp bảo mật trong thiết kế của giao thức này, AODV sẽ được bảo vệ tốt hơn khỏi các nguy cơ bị tấn công. Bài viết này phân tích một số lỗ hổng, đặc biệt là thảo luận về các cuộc tấn công AODV dựa trên thông báo định tuyến. Chúng tôi sẽ trình bày cách xác thực, đảm bảo tính toàn vẹn của thông báo định tuyến và sử dụng tính năng phát hiện xâm nhập dựa trên đặc điểm kỹ thuật để phát hiện các cuộc tấn công vào giao thức AODV.

Từ khóa: *AODV, chuỗi băm, chữ ký số, giám sát mạng, MANET, phát hiện dựa trên đặc tả, phát hiện xâm nhập, SAODV.*

1. INTRODUCTION

Mobile Ad-hoc Network (MANET) (Hasan et al., 2020) is a collection of mobile network nodes that are wirelessly connected to form a temporary network without any support from the network infrastructure, e.g.,

an Access Point. Nodes in an unstructured network act as routers to transport messages to nodes not within their wireless communication range. Because of such capabilities, unstructured wireless networks have many applications, for example, in the military, flood conditions, disasters, etc. Therefore, they must be protected appropriately to achieve reliability, integrity, and high availability.

MANET's features (Suad et al., 2021), such as mobility and collaboration, hinder the network's security. In contrast to wired networks, which have a higher level of security for gateways and routing, unstructured networks have features such as dynamically changing network topology, weak physical interconnection between nodes, no centralized administration, and highly dependent on the cooperation of adjacent nodes (located near each other). Network access control methods like firewalls are not directly applicable, the network structure is constantly changing, and there are no set boundaries for the network. In addition, there is no central administration, making it extremely challenging for the system to encrypt data. A wrong node, meaning a node that has been hacked or infected with malicious code, will easily disrupt the entire network. As a result, unstructured networks are vulnerable to attacks such as eavesdropping, spoofing, packet manipulation, and Distributed Denial of Service (DDoS) attacks.

Security services such as authentication and access control services can enhance the security of unstructured networks (Fazeldehkordi et al., 2015). However, single techniques cannot prevent all attacks (e.g., attackers from obtaining the key used for encryption). Therefore, it is necessary to have other security techniques to deal with nodes with lousy behavior that take over keys and access rights. Intrusion detection techniques that successfully identify attacks with wired networks can also provide additional defense, so intrusion detection and responsiveness are always crucial with many unstructured networks (Rajendra & Shiva, 2022).

Access detection includes the cumulative real-time collection of data from the monitoring system and immediate analysis of such data; this data is logged from an operating system or network packet analysis programs. The techniques involved in access detection are generally classified into three main categories: *signature-based detection*, *anomaly detection*, and *specification-based detection.*

2. AODV ROUTING PROTOCOL PROBLEMS

Many types of attacks can compromise AODV. In this section, we study the typical vandalism in AODV that corrupts the data path. In accordance with our research, we also provide some attack scenarios.

2.1. Overview of AODV

The AODV routing protocol is a stateless and reactive protocol that establishes the desired path of the source node using a Routing Request Message (RREQ) and a Routing Reply Message (RREP) (Singh & Kumar, 2017). When a node wants to find a path to a destination node, it broadcasts an RREQ path request message with a unique ID (RREQ ID) to the surrounding nodes. When a node receives an RREQ message, it updates its SN (Sequence Number) and establishes a reverse path to the source node in the routing table. If this node is the destination node or has a route available to the destination node because of the previous request, it will transmit an RREP reply message back to the source node.

The source node or intermediate node that receives the RREP will update its forwarding path to the destination in the routing table. Otherwise, it continues to broadcast the RREQ message. If a node receives an already processed message, it will ignore and not forward it.

In AODV, the SN sequence number plays an essential role because it indicates the novelty of the routing information and guarantees the absence of repeated paths. The sequence number is only incremented when two conditions are satisfied: When the source node initiates the RREQ and the destination node replies to the RREP. The source node can only update the sequence number. Hop count (HC) determines the shortest path and will be incremented by one each time a node forwards an RREQ or RREP message. When a link is broken, a path error (RRER) packet is propagated to the source node along the established return path, and intermediate nodes delete that input in their routing tables. AODV maintains links with neighboring nodes by periodically sending hello messages.

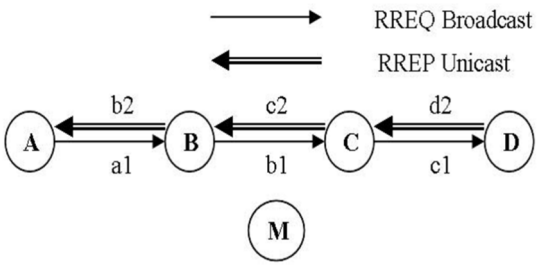

Figure 1. An AODV scenario.

Type	RREQ			RREP		
Msg	a1	b1	c1	d2	c2	b2
IP.Src	A	B	C	D	C	B
IP.Dst	255	255	255	C	B	A
HC	0	1	2	0	1	2
AODV.Dst	D			D		
SN.Dst	0 (Unknown)			61		
AODV.Src	A			A		
SN.Src	100					
RREQ ID	20					

Figure 2. RREQ and RREP values.

Figure 1 depicts the flow of RREQ and RREP messages in an AODV scenario, where node *A* wants to find a way to node *B*. (Initially, nodes *A*, *B*, *C*, and *D* have no path). An RREQ broadcast message (a1) to *B*. *B* further broadcasts the request (b1). *C* receives this message and broadcasts message (c1), reaching destination node *A*. Finally, *D* sends back the RREP message as a unicast message to *A*. We call RREQ packets, and RREP is the request-response flow. The values of the fields in the routing message are recorded as shown in Figure 2.

2.2. Vulnerable fields in AODV control messages

Table 1. Vulnerable AODV packet fields.

Fields	Change when attacked
RREQ ID	Increment to create a new RREQ request
Hop Count	If the sequence number is the same, decrease it to update another node's forwarding table or increase it to drop the updating
IP header and Source IP, Destination IP	Replace it with another IP address or no value
Source and Destination Sequence Number	Increase to update the forward routing table or decrease to drop the update

AODV is vulnerable to falsifying route information by attackers to redirect routes and initiate other attacks. In each AODV routing packet, some required fields, such as the hop count (HC), the source and destination sequence number (SN), the IP header as well as the source and destination IP addresses of the AODV, and the RREQ ID number, are the required for proper protocol implementation. Errors in any of the above fields can also cause AODV to crash. Table 1 records some vulnerable fields in AODV routing messages and their changes when attacked.

An attacker can launch a single attack packet consisting of several cleverly altered fields or a combined attack consisting of multiple attack messages, which is more destructive and lasts longer than a single attack (Sazzat et al., 2019; Trilok & Subhash, 2020). We will briefly go over a few different types of attacks below.

2.3. Single Attacks

Here are some types of single-attacks.

Spoofing Sequence Number

The sequence number indicates the degree of newness of the path to the associated nodes. If an attacker sends out an AODV control packet with a large sequence number impersonating a victim node, it will change the route to this victim node. For example, in the above AODV scenario, if *M* sends an RREQ (*m*1) to *C* with a *SN.Src* sequence number of 200 (>100), it takes over the priority of *b*1. The path from *C* to *A* would go through *M* instead of going to *B*. Node *M* could then control the path between *A* and *D*. As another example, if *M* sent a RREQ to *B* with the sequence number *SN. Dsr* is 100 (>61); it will take precedence through *c*2. *B* will send data through *M* and to *D* instead of to *C*; *M* controls the path from *A* to *D*. This attack can be self-corrected using that protocol when the victim node issues an RREQ or RREP with a larger sequence number of the attack packet.

Spoofing Hop Count

The damage caused by Hop Count (HC) spoofing does not last longer than that caused by sequence number spoofing, but this type of attack is difficult to detect because it is challenging to know the exact *HC* to check the Hop Count. For example, with this type of attack, if *M* sends an RREQ to *C* with *HC*=0 (<1) (assuming *A*), it will take precedence of *b*1, and as before, *M* can control the path. Alternatively, if *M* sends RREP *c*2 to *B* with *HC*=0 (<1) (assuming *D*), it takes over *c*2 priority, and *M* controls the path. This attack will be corrected when the victim node issues a new RREQ and RREP message with a higher sequence number. However, this attack can become very powerful when combined with other attacks to form a composite attack.

2.4. Multiple Attacks

An attacker can combine multiple single attacks to create a more complex or prolonged attack. The following describes some of these attacks.

Man in the Middle Attack

The attacker issues a forged RREQ and RREP to sabotage another node's forwarding table, resulting in a falsified path. The attacker sends RREQ message *m*1 to *C*, same as *b*1, but with a higher number of *SN.Src*, *SN.Src* = 200(>100), gains priority of *b*1, and sends RREP message *m*2 to *B*, same as *c*2 but with *SN.Dst* = 100 (>61) to get priority of *c*2. Next, *C*'s return path is *M* instead of *B*, so *D* and *C* will go to *A* via *M*. Next step, *B*'s forward path is *M* instead of *C*, so *A* and *B* will go to *D* via *M*. From there, *M* can forward falsified packets. Thus, the entire path *ABMCD* has been replaced with *ABCD* (Figure 3).

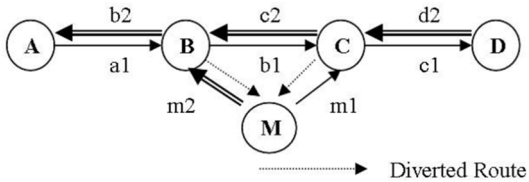

Figure 3. Man-in-the-middle attack.

Tunneling Attack

Two misbehaving nodes perform the tunneling attack, which forges an effective path by creating a tunnel between them. In this way, misbehaving nodes can create paths through them.

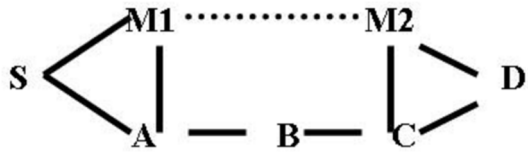

Figure 4. Tunneling Attack.

Figure 4 shows no direct link between *M*1 and *M*2, but *M*1 and *M*2 can pretend to be adjacent by tunneling. *M*1 encapsulates the message, sends it through *A*, *B*, and *C* to *M*2, and pretends to claim a direct path between *M*1 and *M*2. With AODV, when *S* broadcasts an RREQ to *A* and *M*1, it receives an RREP message from *A* and *M*1; their paths are {*S*, *A*, *B*, *C*, *D*} and {*S*, *M*1, *M*2, *D*}. *S* will choose

{*S*, *M*1, *M*2, *D*} but is actually {*S*, *M*1, *A*, *B*, *C*, *M*2, *D*}. *M*1 and *M*2 successfully prevent *S* from choosing the shortest path, {*S*, *A*, *B*, *C*, *D*}. Even encryption-based solutions (Sunitha & Danda, 2021; Ran et al., 2021) cannot resist this attack.

In addition to the above attacks, attacks of pseudo-source node, pseudo-destination, or not forwarding RREQ and RREP messages are also possible.

3. SECURE SOLUTIONS FOR AODV PROTOCOL

In this section, we present an authentication solution using digital signatures and ensuring the integrity of the number of hops over the hash sequence in routing messages for AODV. We also present an algorithm with a tree data structure, which can efficiently detect most malicious attacks in real time with minimal overhead to AODV.

3.1. SAODV protocol

SAODV uses digital signatures to authenticate immutable fields in routing messages and hash strings to protect hop count information (changed during path discovery) (Nurcahyani & Helmi, 2018). The secure AODV protocol extends the routing message by adding several fields, as shown in Figure 5.

The description of RREQ fields:

- *Type*: 64 for RREQ and 65 for RREP
- *Length*: Length of the message excluding Type and Length
- *Hash Function*: The hash function algorithm used
- *Max Hop Count*: The maximum number of hops that can be supported, used to verify the number of hops
- *Top Hash*: The hash value corresponding to the largest number of hops
- *Signature Method*: Algorithm used in digital signature
- *Padding Length*: The length of the stuffed number
- *Public Key*: The public key of the source node that transmits the packet
- *Padding*: Number of extra stuffing
- *Signature*: Digital signature calculated from all unchanged fields of the routing message
- *Hash*: The hash value corresponding to the number of hops at the current node

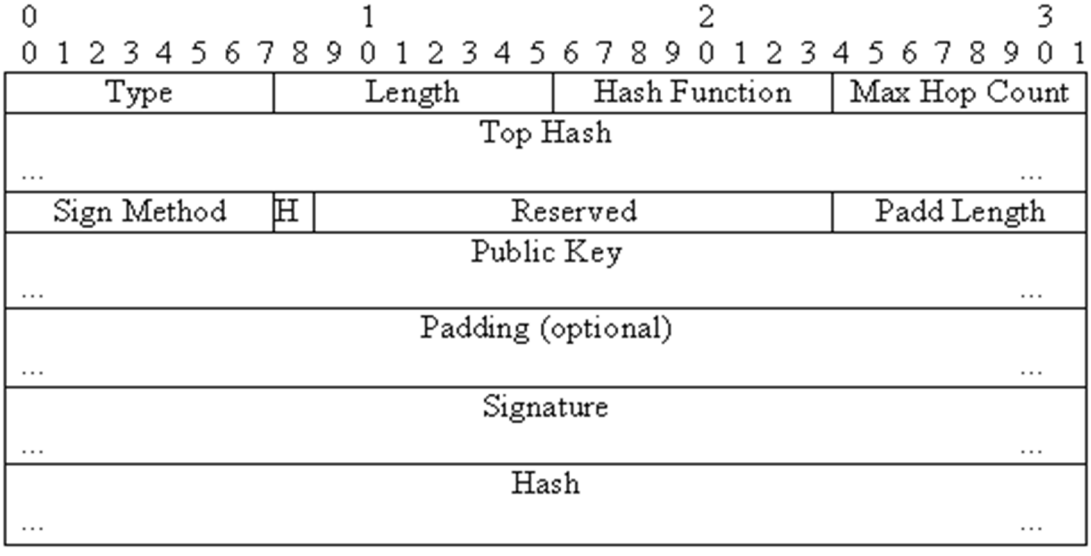

Figure 5. Extended RREQ (RREP) format.

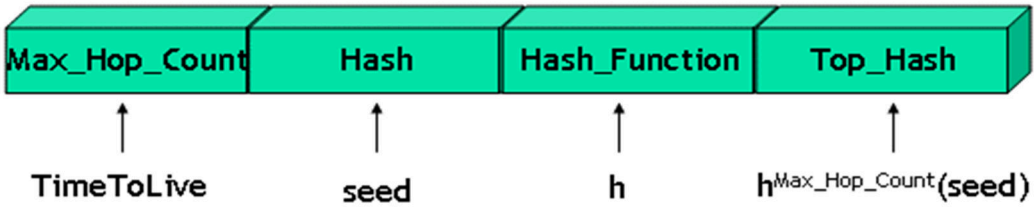

Figure 6. How to calculate the hash at the beginning of the generation of RREQ or RREP.

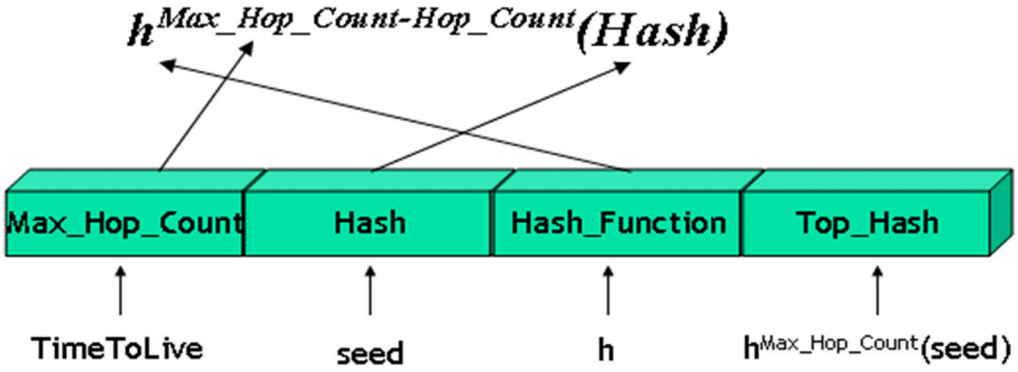

Figure 7. How to calculate the hash at the intermediate node.

Message change field validation: HC value

SAODV uses hash sequences to authenticate the HC of the RREQ and RREP forward between neighboring nodes during route exploration. A hash sequence is formed from a one-way hash function and a random starting value (seed). Whenever a node generates an RREQ or RREP message, the Max Hop Count field is set. The highest hash value (Top Count) is calculated using the hash function "*h*" and a random starting value (Figure 6).

When the node receives the RREQ or RREP, it verifies the hop count as follows: computes the hash h number of times as *n* [*n* = (*Maximum hop count – Number of hops of the current node*)] and compares it with the value contained in the highest hash value (Top Hash) (Figure 7).

After verifying the integrity and authentication, the intermediate node prepares the RREQ or RREP message.

Authentication of immutable fields of messages with digital signature

When a node receives the RREQ for the first time, it verifies the signature before creating or updating a route back to the source node. When the RREQ reaches the destination node, the RREP is sent with an RREP signature. When a node receives an RREP, it verifies the signature before creating or updating a route to the source node. Only when the signature is verified does the node save the route with the signature of the RREP and the expiration time.

When the route probe is successful, the source and destination nodes will communicate along the found routes. If a broken link occurs in the network, a route error message RERR (Route Error) is generated, as shown in AODV. RERR is also protected by digital signature.

3.2. Specification-based AODV monitoring

Specification-based monitoring compares the behavior of objects with their associated security specifications, preserving the correct functioning of the objects. These specifications are usually built-in detail based on security policies, object functions, and usage requirements. Specification-based

detection is not intrusion detection directly – instead, it detects the effect of intrusions similar to instantaneous violations as described in the specifications. As far as the specification is concerned with the correct behavior of objects, specification-based detection by itself is not limited to detecting only known attacks. Typically, a specification for a network protocol forces messages to be exchanged according to network nodes. The specifications will limit how messages are exchanged (e.g., an ACK followed by an SYN) and the content of the messages. These specifications can also be derived from some desired global invariants about the protocol.

In applying the specification techniques for monitoring AODV, we will focus first on the routing messages that were exchanged during the discovery of routes step. In each case, we will track all RREQ and RREP messages in a request-response flow from a source (sending) node to a destination (receiving) node and back to the originating source. This type of specification requires that all nodes send RREQ and RREP messages depending on the protocol specifications, the Hop Count value, RREQ ID, and Sequence Number are correct. In the following, we describe how to monitor a request-response flow using distributed network monitors (NM).

3.2.1. Some basic assumptions

1) All wireless nodes' MAC addresses and IP addresses are registered on the network monitors and maintained unchanged.

2) MAC addresses cannot be spoofed.

3) All network monitoring and its messages are secure and authenticated.

4) Every node must forward or respond to protocol-based messages within a finite number of time cycles.

5) Network monitors are carefully selected to cover all nodes and perform all necessary functions.

6) If a node is out of range of a network monitor, it must be within range of "neighboring monitors."

7) If some nodes do not respond to broadcast messages, this will not cause too serious problems.

3.2.2. Instant monitoring of request-response flows

The nature of ad hoc networks is to prevent any single node "intent" from observing all request-response messages. Therefore, distributed network monitors must monitor RREQ and RREP messages in a request-response flow (starting now referred to as NMs – Network Monitors).

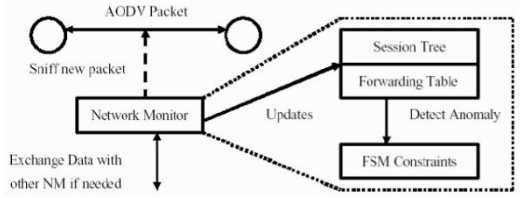

Figure 8. Network monitoring architecture.

Figure 8 illustrates the architecture of a network monitor (NM). The NM directly listens for AODV routing messages and detects faulty RREQ and RREP messages. Messages are grouped based on which request-response flow they belong to. The RREQ ID, source, and destination IP addresses can uniquely identify a request-response flow. An RREQ or RREP message can map to a request-response flow based on the following fields:

- RREQ: source AODV address and RREQ ID
- RREP: source and destination AODV addresses

An NM keeps track of the last received RREQ and RREP messages by each monitored node and maintains the forwarding table of each monitored node. Furthermore, each request-response flow can have several "branches" – RREQ is a broadcast message, and more than one neighbor can continue to broadcast it – NM maintains a "session tree" to keep track of the "branches". When the

NM sees an AODV packet as the current packet, the NM searches the session tree to find the previous packet of this packet. If the NM cannot find the previous packet to match the current packet in the session tree, it asks the neighboring NMs to find it. If one of the neighboring NMs replies, the NM receives information about the packet to look for and the tree in which it resides.

On the other hand, NM would consider it an "active forge anomaly." After comparing the current packet with the previous packet, the NM inserts the current packet into the session tree instead of the next current packet. If it is an RREP message, the NM will mark the new link as a "red link." In addition, NM will update its forwarding table by tracking the session tree. NM can easily match current and forward packets to detect anomalies, especially in RREQ.

Furthermore, the NM can detect incorrect hop counts and their previous nodes in the RREQ. The NM can also identify the broken links of the respective RERRs, which in turn can mark the broken links and notify its nodes not to use these links for some time. Even NM can flag poor-quality nodes from a poor connection and issue many RERRs.

The bandwidth overhead is generated by the NMs when it needs to ask the neighboring NMs for information about the nodes out of their transmission range. This situation occurs when nodes move out of range of an NM, or a packet is forwarded to a node out of transmission range.

4. CONCLUSION

In our research, we have described the AODV protocol overview and proposed a solution to authenticate, ensure the integrity of routing messages, and use specification-based access detection to detect AODV protocol attacks. However, the limitation of our study is that due to limited time, the proposed solution has not been evaluated effectively by popular methods such as modeling, simulation, or emulation on real systems (testbeds). These works will be studied in the near future. In addition, the next development step might be to evaluate the security of the protection solutions and the impact of those solutions on the performance of the AODV protocol in wireless ad hoc networks.

ACKNOWLEDGMENT

This research was supported by the Vietnam Academy of Science and Technology (VAST) under a project numbered "VAST01-09/22-23".

REFERENCES

Fazeldehkordi, E., Sadegh, A., I., & Akanbi, O. (2015). *A Study of Black Hole Attack Solutions on AODV Routing Protocol in MANET*. Imprint: Syngress.

Hasan, M., Z., Hussain, M., Z., & Ullah, Z. (2020). Mobile Ad-Hoc Networking (MANET). *Journal of Computer Science, 3,* 9-18.

Nurcahyani, I., & Helmi, H. Performance Analysis of Ad-Hoc On-Demand Distance Vector (AODV) and Dynamic Source Routing (DSR) Under Black Hole Attacks in Mobile Ad Hoc Network (MANET). *International Symposium on Electronics and Smart Devices (ISESD) (2018),* 1-5.

Rajendra, P., & Shiva, S. (2022). Secure Intrusion Detection System routing protocol for mobile ad-hoc network. *Global Transitions Proceedings, Volume 3, Issue 2, November 2022,* 399-411. DOI: 10.1016/j.gltp.2021.10.003.

Ran, C., Yan, S., Huang, L., & Zhang, L. (2021). An improved AODV routing security algorithm based on blockchain technology in ad hoc network. *EURASIP Journal on Wireless Communications and Networking, 52* (2021). DOI: 10.1186/s 13638-021-01938-y.

Sazzat, H., Md.Sazzad, H., Romana, R., E., Songita, D., Suborna, S., & Tajul, I.

(2019). Detecting Black hole attack by selecting appropriate routes for authentic message passing using SHA-3 and Diffie-Hellman algorithm in AODV and AOMDV routing protocols in MANET. *10th International Conference on Computing, Communication and Networking Technologies (ICCCNT) (2019),* 1-7. DOI: 10.1109/ICCCNT 45670.2019.8944395.

Singh, M., & Kumar, S. (2017). A Survey: Ad-hoc on-Demand Distance Vector (AODV) Protocol. *International Journal of Computer Applications, 161*(1), 38-44. DOI: 10.5120/ijca2017913109.

Suad, A., A., Alyaa, A., A., & Enas, F., A. (2021). Mobile ad hoc network (MANET) proactive and reactive routing protocols. *Journal of Discrete Mathematical Sciences and Cryptography, Volume 24, 2021 – Issue 7,* 2017-2025.

Sunitha, S., & Danda, B., R. (2020). On the Elliptic Curve Cryptography for Privacy-Aware Secure ACO-AODV Routing in Intent-Based Internet of Vehicles for Smart Cities, in *IEEE Transactions on Intelligent Transportation Systems, Volume 22, No. 8*, 5050-5059. DOI: 10. 1109/TITS.2020.3008361.

Trilok, K., S., & Subhash, C., S. (2020). Recent advancements, review analysis, and extensions of the AODV with the illustration of the applied concept. *Ad Hoc Networks, Volume 103*, 102148. DOI: 10.1016/j.adhoc.2020.102148.