A Comprehensive Review on Lightweight Security Mechanisms to Mitigate Network Layer-Based Active Attacks

Uthumansa Ahamed[1], and Shantha Fernando[2]

[1]*Department of Information and Communication Technology, Faculty of Technology, South Eastern University of Sri Lanka, Sri Lanka*
[2]*Department of Computer Science & Engineering, Faculty of Engineering, University of Moratuwa, Sri Lanka*

[1]urmail2ahmed@gmail.com, [2]shantha@cse.mrt.ac.lk

Abstract
Node mobility, infrastructure-less network, open network boundary, and limited resources are general characteristic features of a Mobile Ad-hoc Network (MANET). These characters open MANETs to many security attacks. Network layer-based active attacks such as black-hole and gray-hole attacks are common and destructive. Proposed solutions for these attacks failed to perform well. Some mechanisms that are used in an infrastructure-based network were proposed as lightweight security mechanisms for MANETs. One hundred and two reputed journal and quality conference papers were selected for the review. In this paper, we comprehensively reviewed available security solutions, including lightweight solutions on MANET. The review proved that there is a demand for a lightweight security solution capable of operating with limited resources and mitigating active attacks without a performance drop.

Keywords: Active, Blackhole, Grayhole, Lightweight, Review, Security

I. INTRODUCTION

Mobile Ad-hoc Network (MANET) is a type of Ad-hoc Network. Node mobility is the main character in MANETs. Therefore, network topology changes frequently. Few basic characters are common to MANET. These are mobile nodes, infrastructure-less network nature, open network boundary, and limited resources. These features provide advantages such as the instant formation of the network in hostile conditions (natural disasters, war, etc) where the services of the infrastructure-based networks are unavailable. Moreover, MANETs are used for commercial purposes such as virtual classrooms. Security threats and attacks are the main drawbacks of MANETs due to these main characters. Black-hole attacks are common and destructive security attacks on MANETs. Numerous amounts of security solutions were proposed to mitigate the black-hole attacks. Moreover, lightweight security mechanisms were proposed by referring to the security techniques that were applied on infrastructure-based networks such as cryptography; nevertheless, available solutions are not effective enough to fit the MANETs. Therefore, in this paper, lightweight and proposed security mechanisms to mitigate black-hole attacks were reviewed to identify the research gap on widespread lightweight security mechanisms to mitigate black-hole attacks. The rest of the paper is organized as follows. The available review papers were reviewed in Section II, and the methodology was described in Section III. Section IV describes the general features of MANETs in detail. Section V presents the routing protocols in MANET. The network layer-based security attacks were described in detail in Section VI. The factors that are used to evaluate the network performance are discussed in Section VII. The available security solutions were presented in Section VIII, and lightweight security solutions were presented in Section IX, and the conclusion of our research is presented in Section X.

Khanna and Sachdeva (2019) presented a comprehensive review of available security mechanisms for black-hole attacks and their variants. The paper contained a review, summary, and discussion in it. The authors identified a few research gaps, and the main research gap was a lightweight mechanism. They failed to consider existing lightweight security mechanisms in their study. In separate two different research (Gurung & Chauhan, 2017: Kahn & Jamil, 2017) presented an analysis and a summary of available black-hole attack mechanisms. The review was based on a limited amount of literature. In 2014, Mitchell & Chen surveyed intrusion detection in wireless

network applications. The survey presented a quality analysis and review of the available security mechanisms. The concepts of lightweight security mechanisms have been proposed for the last few decades, though these mechanisms are not reviewed. These types of mechanisms are based on the compatible modification of infrastructure-based security mechanisms applied to MANETs. Therefore, these mechanisms should be reviewed to find a suitable solution for network layer-based active attacks.

II. METHODOLOGY

The research articles were searched on the official websites of reputed journals and conferences. "Active attacks", "MANET", "Mobile Ad-hoc Network", Mechanism", "Review", "Security", and "Survey" were a few keywords that were used to search articles. Individual or combination of keywords used for the searches. The full papers of the relevant articles were downloaded from the search results based on the research title. The following reasons were used to filter downloaded articles from the review as illustrated in Figure 1.

- Article language – not English
- The contradiction between the theory and the presented results
- Unclear results
- Articles with duplicated works

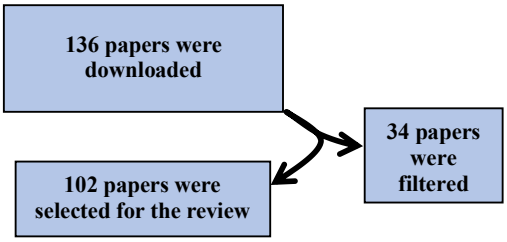

Figure 1: Filtering of articles for the review

III. RESULTS AND DISCUSSION

A. General Features of A MANET

Few features are general to a MANET. These features are being considered as the main factors that are listed as follows.

1) Mobility

The most unique feature and the critical factor (Rangaraj & Anitha, 2017) in the MANET is node mobility. This will decide the network topology. Though a source node is managing the maintenance of the network connectivity by allowing mobile nodes to join the route after existing links are broken, the node mobility creates an opportunity for the source node to find the shortest path to the destination node after the breakage of the existing route (Ahamed & Fernando, 2021).

2) Infrastructure-less network

MANET follows the peer-to-peer networking concept to establish communication. Therefore, it does not depend on any network infrastructure. The source node selects any neighbour node that helps to find a route to the destination node. Nodes are capable of restoring network connectivity when a node is left from the network. Then source node initiates to reestablish the connectivity by selecting other nodes. Therefore, the infrastructure-less nature of the network helps to stay connected.

3) Limited Resources

Nodes are designed to allow nodes to be mobile. Therefore, nodes are designed with limited resources: energy source, computing or processing power, memory, storage capacity, node size, and weight. Another important limited resource is the wireless radio range. Therefore, the source node is forced to depend on the help of the neighbour nodes for communication.

4) Open network boundary

The limited radio range of nodes enforces the source node to depend on the help of the neighbour nodes to communicate. Node mobility disrupts communication by breaking the link between nodes. A route reconstruction mechanism is used to prevent communication loss. Therefore, MANET maintains an open network boundary to overcome this issue. Therefore, a node can join or leave the network without any constraints. This concept helps restore collapsed networks.

B. Routing Protocols

Routing protocols are used to find the route between source and destination nodes when these nodes are unreachable within their radio transmission range (Ahamed & Fernando, 2020). A routing protocol is one of the protocols operating on the network layer (Dawoud et al., 2011) in the OSI model. Generally, routing protocols can be divided into two broad categories based on their operational mechanism. Those are Proactive and Reactive Routing Protocols.

1) Proactive Routing Protocols

In proactive routing protocols, the route details are updated periodically to maintain the route information in a table which is called a routing table. This periodic updating of the route details continues even when there is a demand for a route or not. Therefore, these types of routing protocols consume more node energy to operate. These protocols are only suitable for networks in which node energy is not considered a critical factor such as wireless sensor networks with few nodes. Examples of these types of protocols are:

Ex.:
Destination-Sequenced Distance Vector Protocol (DSDV),
Cluster-head Gateway Switch Routing (CSGR).

Ex.:
Ad hoc On-Demand Distance Vector (AODV),
Dynamic Source Routing (DSR),
Temporally Ordered Routing Algorithm (TORA),
Scalable Source Routing (SSR)

According to the summary in Table 1, reactive routing protocols are more suitable for MANETs than proactive routing protocols. Out of available reactive routing protocols, AODV and DSR perform well as stated in Table 2. In DSR, the route information is maintained in the source node. Similarly, each data packets hold the entire route details on it. Therefore, DSR fails to operate at the higher numbers (Sharma et al., 2015, Kanthe et al., 2012) of nodes in the network. Moreover, node mobility changes network topology frequently in a MANET. Therefore, a routing protocol should be capable of handling the failure of links between nodes and node mobility (Shahzamal, 2018). AODV uses only the destination IP address and sequence number to locate the destination node. Moreover, the AODV routing protocol is equipped with features to overcome link failures due to node mobility through local route repair mechanisms.

Table 1: Comparison between proactive and reactive routing protocols

	Proactive Routing Protocols	**Reactive Routing Protocols**
Mobility	Network collapse (Sharma & Kumar,2016).	Capable to manage (Ahamed & Fernando 2021: Schellenberg, 2020)
Number of nodes in the network	Only suitable for a few nodes (Bai et al., 2017)	Scalable from few to higher numbers (Sharma & Kumar 2016)
Network Overhead (NO)	Periodic communication causes high NO (Chavan et al., 2016)	Lower than proactive (Semary & Diab, 2019: Rangaraj & Anitha, 2017)
RO	Periodic acknowledgements cause high RO(Reddy, 2018: Bai et al., 2017: Chavan et al., 2016: Sharma & Kumar, 2016)	Nodes are idle when there is no communication (Perking et al., 2003).
Energy Consumption	Require uninterrupted energy (Reddy, 2018: Rangaraj & Anitha, 2017)	Only active for communication (Boukerche et al., 2011: Perking et al., 2003).
Network Performance	High only in a lower number of nodes. (Bai et al., 2017: Boukerche et al., 2011: Nand et al, 2010)	Fair in a lower number of nodes on high in a higher number of nodes, (Bai et al., 2017: Chavan et al., 2016: Sharma & Kumar 2016)
Connectivity	Initiation is quick (Semary & Diab, 2019: Boukerche et al., 2011)	Start to initiate when there is a demand (Perking et al., 2003)

2) Reactive Routing Protocols

These types of protocols establish a route from a source node to the destination node only when there is a demand for a route. The source node starts to broadcast routing request packets to find a route to the destination node when there is a demand. Routing request packets are sent to the neighbour nodes, and if a routing request is received from a node, it will retransmit the packets until the request is received by the destination node. After a successful route discovery, the source node starts communication with the destination node by forwarding data packets. Examples of these types of routing protocols are:

Table 2: Reactive routing protocols comparison (Reddy et al., 2018: Sooriyaarachchi, 2016: Kaur et al., 2013)

Protocol	Route Selection	Route	Method	Loop free
AODV	Shortest and most updated path	Multiple	Unicast	Yes
TORA	Shortest path	Multiple	Broadcast	No
DSR	Shortest and most updated path	Multiple	Unicast	Yes
SSR	Associativity and Stability	Single	Broadcast	Yes

(Perking et al., 2003). Therefore, AODV performs well in MANET than DSR (Reddy et al., 2018: Bai et al., 2017: Sooriyaarachchi, 2016: Sharma, and Kumar, 2016: Sharma et al., 2015: Kanthe et al., 2012).

C. *SECURITY ATTACKS*

Security attacks are not only from outside the network; compromised nodes also engage in different types of attacks in the network (Reddy et al., 2021: Teodoro et al., 2014) even after a successful route formation. The most common network layer-based security attacks on a MANET can be categorized into two: Active attacks and Passive attacks.

1) *Active attacks*

Active attacks are a type of attack which disrupts the network operation. These types of attacks impact the network performances seriously. Finally, it will collapse the network. These types of attacks are possible from the outsiders of the network as well as from the compromised nodes. Therefore, for the fair operations of the network, these types of attacks should be handled. Examples of these types of attacks are the Black-hole and Grayhole attacks. These attacks can be simulated (Ahamed & Fernando, 2021b) in network simulators.

1) *Black-hole attack*

A Black-hole attack is a type of denial-of-service attack. These attacks drop data packets in an abnormal amount than normal nodes in the network. A Black-hole attack is classified as a network layer-based Active attack. During the route-finding process of a routing protocol, the attacker node waits to receive a request from a source node. Then it starts replying by advertising itself as it has the destination node as its neighbour. A malicious node injects false information (Dorri et al., 2015: Casado et al., 2014), claiming that it has the shortest and newest route to the destination node. As illustrated in Figure 2, a black-hole node is possible to establish a route to the destination node or no possible route. The reply from the malicious node reaches the source node at first other than a reply from a non-malicious node is reached.

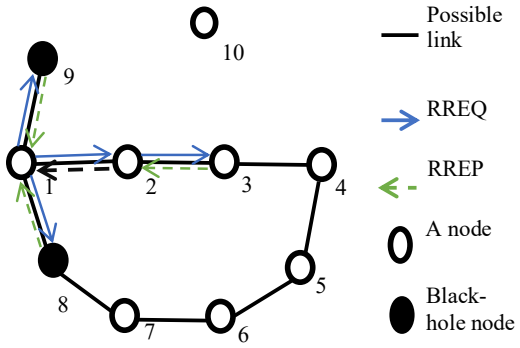

Figure 2: An example of black-hole attacks

Table 3: A description of NPMs

	PDR	AEED	Throughput
Description	the ratio between the total number of packets sent by the source node and the total number of packets received by the destination node	an average amount of time that is taken by a data packet to reach the destination node from the source node	a ratio between the total number of packets received by the destination node and the total time to receive all packets
Unit	Percentage	Seconds	Bytes per seconds

The source node misleads to consider the reply of the malicious node. Finally, the source node is considered the reply from the malicious node because it seems to be the shortest and newest

Therefore, it starts to send the RREP packet to the source by increasing the destination sequence number by one. Then 2 retransmits the same RREP packet to the destination node by increasing

Table 4: Summary of security mechanisms and the publications

Mechanisms based on	Description	Examples
Trust	It is used to evaluate the neighbour nodes. It is updated based on the performance of a node.	Mahamune & Chandane, 2021: Mukhedkar & Kolekar, 2019: Movahedi & Hosseini, 2017: Sethuraman & Kannan, 2017: Khanna, 2016: Xia. et al., 2015: Hinge & Dubey, 2016: Vijayakumar et al., 2015: Subramaniyan et al., 2014
Validation of threshold value	Sequence numbers or other values related to the routing or data in the network were validated to detect the attacker.	Reddy et al., 2021: Elmahdi et al., 2020: Shrestha et al., 2020: Hammamouche et al., 2018: Gurung & Chauhan, 2017: Poongodi & Karthikeyan, 2016: Panos et al., 2016: Patel & Chawd 2015: Kumar & Kumar, 2015: Salunke & Ambawade, 2015: Jhaveri & Patel, 2015: Casado et al., 2015
Detection and prevention	Behavioural patterns, filters, fuzzy logic, or logical inference are used on a neighbour node to differentiate attackers from other nodes.	Pandey & Singh, 2020: Kalkha et al., 2019: Moudni et al., 2019: Hammamouche et al., 2018: Rmayti et al., 2017: Khanna. N., 2016: Usha et al., 2016: Arthur & Kannan, 2015: Balan et al., 2015: Nadeem & Howarth, 2014: Casado et al.: 2014: Nadeem & Howarth, 2013: Olmos et. al., 2012: Joseph et al., 2010: Sen et al., 2007:
Collaboration	Data-link layer and network layer or all the nodes on the network or set of nodes in the network or set of groups in the network are worked collaboratively to identify attackers based on the routing and data packet information.	Usha et al., 2016: Singh & Singh, 2016: Subba et al., 2016: Arathy & Sminesh, 2016: Arthur & Kannan, 2015: Funde & Chandre, 2015: Poongodi & Bose, 2015: Sharma, 2015: Shi et al., 2014: Deb et al., 2014: Zadeh & Kabiri, 2014
Separate packets	Separate acknowledgement packet or modification on available routing packets used to collect information to detect attacker node.	Pathan et al., 2019: Dorri et al., 2017: Chavan et al., 2016: Dorri, 2016: Babu & Usha, 2016: Patel & Chawd, 2015: Ahmed et al., 2015: Rana et al., 2015: Dhaka et al., 2015: Basabaa et al., 2014: Shakshuki et al., 2013: Sun et al., 2012
Special hardware	Special hardware components are used to collect the information to detect attacker nodes.	Song et al., 2008
Collective mechanisms	Two or more mechanism works together to detect an attacker.	Ourouss et al., 2020: Singh et al., 2018: Anusha & Sathiyamoorthy, 2017: Akbani et al., 2012

route. It assumes that it can create a route to the destination node through the malicious node. Therefore, the source node starts the communication by sending data packets to the malicious node. The malicious node drops all.

Data packets (Semary & Diab, 2019: Casado et al., 2014) that are received from the source node, though it allows only routing packets. For example, if 1 is a source node that needs to send data packets to destination node 4, it starts to send RREQ packets. The packets will reach neighbour nodes of the 1. According to Figure 2, nodes 9, 2, and 8 are neighbours of 1. The 2 does not have 4 as its` neighbour. Therefore, it rebroadcasts the RREQ packet to its neighbours by increasing the source sequence number by one. Then, 3 receives the RREQ packet, and it has 4 as its` neighbour.

the destination sequence number by one. This is the formal process of the AODV routing protocol in a MANET, nevertheless, black-hole nodes act differently than usual. When 8 and 9 receive the RREQ packet, they replace the destination sequence number with a higher possible integer value and send the RREP, though there is a possible route to the destination node (via 9 or not).

2) Grayhole attack

The grayhole attack can be described as an extension of the Black-hole attack (Jain & Raghuwanshi, 2014). A grayhole attack is classified as a network layer-based Active attack. A malicious node can maintain states during a communication either by behaving as a genuine

node or by behaving as a malicious node. Malicious nodes use true data to reply to a route request during the route-finding process of the routing protocol. Though, during communication between a source node and a destination node, the attacking node acts as a genuine node by delivering or retransmitting what it received. After some period, it starts to drop all the data packets that it receives (Ibrahimet al., 2015). In some other cases, a malicious node drops all the data packets from a specific node in the route and forwards or retransmits data packets from other nodes. As an example, in Figure 2, if 8 and 9 are normal nodes, then the route between 1 and 4 will be 1, 2, 3, and 4. If 2 is a grayhole node, then it will cooperate to find the route. The grayhole node starts to drop all data packets after some period, or it will drop all the data packets from a specific node.

D. NETWORK PERFORMANCE MATRICS

Network Performance Metrics (NPM) is a set of measurements of a network that is used to understand the performances of a network. The values of these NPMs are based on the packets that are transmitted through the network during communication between nodes. PDR, AEED, and Throughput are some examples of formal NPMs as described in Table 3.

E. AVAILABLE SECURITY SOLUTIONS

Researchers proposed a huge number of security mechanisms, as presented in Table 4 to detect or prevent or mitigate black-hole attacks in a MANET. Some mechanisms are capable of performing all of these operations. Most of the mechanisms are based on the specific routing protocol. Some researchers proposed individual mechanisms for each security attack, though some researchers proposed a system to handle a single attack or else to handle the number of attacks at once. The taxonomy of the available security mechanisms can be categorized as follows based on the available review studies (Khanna & Sachdeva, 2019: Khan & Jamil, 2017: Gurung & Chauhan, 2017: Dubey & Saxena, 2016: Mitchell & Chen, 2014: Boukerche et al., 2011).

F. LIGHTWEIGHT SECURITY SOLUTIONS

The fundamental features of the MANET prevent the usage of the quality security countermeasures that are used in infrastructure-based networks, such as cryptography and IDS. Some researchers proposed (Shukla et al., 2021: Pandey & Singh, 2020: Moudni et al., 2019: Khanna. N., 2016) these mechanisms for MANETs. As presented in Table 5, these mechanisms are capable of handling security threats in only some instances due to their complex nature.

Table 5: Lightweight security solutions

Author/s	Description	Advantages of the lightweight concept
Ahamed & Fernando, 2022	Lightweight Security Mechanism to Mitigate Active Attacks in a Mobile Ad-hoc Network	Relatively same performance compared to the network without an attack
Liu et al., 2021	A computing model based on a lightweight framework is proposed to reduce the computing pressure of edge nodes.	More secure edge node environment and guaranteed security of the user's privacy data
Batra et al., 2021	A new hybrid lightweight (key size, and mechanism) logical security framework for offering security in IoT	Comparatively fast making the compromise of keys
Lee & Chen, 2021	Lightweight cryptographic operations, including a one-way cryptographic hash function, the Barrel Shifter Physically Unclonable Function	Provide more security than related schemes but also are more efficient.
Wang et al., 2021	A lightweight blockchain-based secure routing algorithm for swarm UAS networking	Reduce the routing consumption
Gaurav & Singh, 2021	A secure lightweight backbone construction approach for MANET	A high degree of detection rate without bringing in any significant traffic
Santos et al., 2020	Proposed a Federated Lightweight federated identity authentication protocol exclusively tailored to IoT	Reduced data exchange overhead, storage, memory, and computation time
Jamshidi et al., 2020	A lightweight algorithm using watchdog nodes	False detection probability and imposing ignorable processing and memory overhead.
Kumar et al., 2020	A lightweight signcryption (hash function) scheme for perception layer devices in IoT	Reduced communication cost and energy consumption, less complex and fast performance
Wen et al., 2020	Proposed aggregate signature schemes for lightweight devices (Healthcare Wireless Medical Sensor Networks)	Quick verification of multiple messages

Ayobi et al., 2020	A lightweight blockchain-based decentralized trust model for preserving the privacy in VANET	Deal with imprecise data in VANET
Conti et al., 2019	A lightweight mechanism and practically feasible countermeasures against two different types of DDoS attacks	Adequate reduction in bandwidth consumption and processing delay of new request
Hammamouche et al., 2018	A lightweight reputation-based approach to detect single and cooperative black-hole attacks	High delivery and the detection rates of packets and low communication overhead
Shahzamal, 2018	Lightweight Mobile Ad-hoc Network Routing Protocols for Smartphones	Node mobility causes high control overheads.
Xia et al., 2016	A lightweight routing protocol to provide a feasible approach to choosing an optimal two-way trusted route	Consumes limited computational resources and reduces the RO
Suraj et al., 2015	A novel approach to mobility prediction using movement history and existing concepts of genetic algorithms	A faster rate of mobility prediction
Martirosyan & Boukerche, 2015	A new encryption scheme which is lightweight in computation by leveraging network coding	Minimal energy consumption and low encryption time
Wang et al., 2014	A lightweight Proactive Source Routing protocol that can maintain more network topology information than DSR	Smaller overhead and better data transportation performance
Cheng et al., 2014	Delivery-guaranteed location-free routing protocol with a lightweight construction cost	Good performance in construction message overhead, the maintenance time and message overhead, and the great PDR
Zhang et al., 2013	New encryption scheme which is lightweight in computation by leveraging network coding	Reduce energy consumption, lower encryption time of P-Coding
Marchang & Datta, 2012	A lightweight IDS is used for estimating the trust of nodes	Consumes limited computational resources
Zhang et al., 2012	A group-based lightweight authentication scheme	The authentication time is minimized and the fast MAC layer handoff is achieved, no extra overhead is introduced.
Malekzadeh et al., 2011	A lightweight non-cryptographic security solution is proposed to prevent wireless DoS attacks.	It prevents wireless DoS attacks, and the security cost is not remarkable with the simplicity of the overall computation.
Babu & Selvan, 2010	A lightweight and Attack Resistant Authenticated Routing Protocol for MANETs	A high PDR with reduced the delay and overhead and detects the malicious nodes quickly
Tran et al., 2009	A Bloom filter-based beaconing mechanism to aggregate and distribute information for presence detection	Minimized communication overhead, and speedy information propagation
Song et al., 2009	The proposed protocol has strengths such as light computational load, backward compatibility, and dependable operation.	Minimal computational overhead, low computational cost and minimal delay
Wool, 2005	A lightweight solution to the host-revocation problem	Simple, very efficient, uses well-understood key transport protocols and cryptographic primitives, requires no additional equipment

These mechanisms require high computational power, higher storage, uninterrupted battery backup, and infrastructure-based network topology. Therefore, these mechanisms barely fit MANET. If these mechanisms need to be applied in MANET, then those mechanisms should undergo serious modifications that enable them to fit into the MANETs. Then these modified mechanisms are called lightweight mechanisms in terms of specific concern as summarized in Table 5. The processing time or delivery time or delay or EED or AEED and the performance of the other relevant factors such as throughput, and PDR are used to consider the mechanism as a lightweight mechanism.

IV. CONCLUSION

The following research gaps were identified by reviewing the works of literature.

- Active attacks are destructive and commonly available among the reactive routing protocols. AODV is a suitable routing protocol for MANETs. Routing protocols should undergo serious modification to handle data security including routing.

- Available security solutions for the active attacks failed to perform well than the performance of the

network without the attack. Therefore there is a demand for a lightweight security solution that is capable of operating with limited resources and mitigating active attacks without a performance drop in common NPSs.

Network layer-based active attacks are common and destructive in action. Black-hole attacks are a general example of these types of security attacks. Many solutions to mitigate black-hole attacks have been proposed in the last few decades. Some solutions were oriented to the mechanisms that were used for the infrastructure-based security mechanism. These mechanisms were modified to apply to MANETs as lightweight mechanisms though these were performance dropped the same as standard security mechanisms do. Moreover, some of these lightweight mechanisms introduced new NPSs that decrease the network performance such as more energy consumption and false detection. Therefore, the routing protocol should be modified to handle network layer-based security attacks too, or proposed lightweight security solutions should be widespread and capable of operating in minimum resources without a performance drop.

REFERENCES

Ahamed, U. and Fernando. S. (2020) “Identifying the Impacts of Active and Passive Attacks on Network Layer in A Mobile Ad-hoc Network: A Simulation Perspective”, *in International Journal of Advanced Computer Science and Applications*, Vol. 11(11), 2020. doi:10.14569/IJACSA.2020.0111173

Ahamed, U. and Fernando, S. (2021a) “Identifying the Impacts of Node Mobility on Network Layer Based Active and Passive Attacks in Mobile Ad Hoc Networks: A Simulation Perspective”.

Chaubey, N., Parikh, S., and Amin, K. (ed.) Computing Science, Communication and Security. COMS2 2021. *Communications in Computer and Information Science*, Springer, Singapore. doi:10.1007/978-3-030-76776-1_18

Ahamed, U. and Fernando, S. (2021b) “Simulation of Network Layer-Based Security Attacks in a Mobile Ad-hoc Network”, *in Journal of Information Systems & Information Technology (JISIT*), 6(1), 2021; pp 28- 42, SEUSL

Ahamed. U. and Fernando. S. (2022) "Lightweight Security Mechanism to Mitigate Active Attacks in a Mobile Ad-hoc Network", *in International Journal of Electronics and Telecommunications*, 2022, Vol. 68(1), pp. 145–152. doi:10.24425/ijet.2022.139862

Ahmad. S.J., Reddy. V.S.K., Damodaram. A. and Krishna. P.R. (2015) "Detection of black hole attack using code division security method", *in: Emerging ICT for Bridging the Future-Proceedings of the 49th Annual Convention of the Computer Society of India CS*I

Akbani. R., Korkmaz. T. and Raju. G.V. (2012) "EMLTrust: An enhanced Machine Learning based Reputation System for MANETs", *in Ad Hoc Networks,* Vol. 10(3) 2012, pp. 435-457. doi:10.1016/j.adhoc.2011.08.003

Anusha. K., and Sathiyamoorthy. E. (2017) "A new trust-based mechanism for detecting intrusions in MANET", *in Information Security Journal: A Global Perspective,* Vol. 26:4, pp. 153-165. doi:10.1080/19393555.2017.1328544

Arathy, K.S.,and Sminesh, C.N. (2016) “A Novel Approach for Detection of Single and Collaborative Black Hole Attacks in MANET”, *in Procedia Technology,* Vol. 25, pp. 264-271, Elsevier.doi:10.1016/j.protcy.2016.08.106

Arthur. M.P., and Kannan. K. (2016) "Cross-layer based multiclass intrusion detection system for secure multicast communication of MANET in military networks", *in Wireless Networks*, 2016 22(3), pp. 1035-1059, Springer. doi:10.1007/s11276-015-1065-2

Ayobi. S., Wang. Y., Rabbani, M., Dorri. A., Jelodar. H., Huang. H., and Yarmohammadi. S. (2020). "A Lightweight Blockchain-Based Trust Model for Smart Vehicles in VANETs", in Wang. G., Chen, B., Li. W., Pietro D.R., Yan. X. and Han. H. (Eds) Security, Privacy, and Anonymity in Computation, Communication, and Storage. SpaCCS 2020. *Lecture Notes in Computer Science*, Vol. 12382. Springer. doi:10.1007/978-3-030-68851-6_20

Babu. M.R., and Selvan. S. (2010) "A lightweight and attack resistant authentication routing protocol for mobil adhoc networks", *in International Journal of Wireless & Mobile Networks (IJWMN*), Vol. 2(2), 2010. doi:10.5121/ijwmn.2010.2202

Babu. M.R., and Usha. G. (2016) "A novel honeypot based detection and isolation approach (NHBADI) to detect and isolate black hole attacks in MANET", *in Wireless Personal Communications 2016* 90 (2), pp. 831–845, Springer. doi:10.1007/s11277-016-3229-5

Bai. Y. Mai. Y. and Wang. N. (2017) “Performance comparison and evaluation of the proactive and reactive

routing protocols for MANETs," *in 2017 Wireless Telecommunications Symposium (WTS), Chicago, IL, USA: IEEE*, 2017, pp. 1-5

Balan. E.V., Priyan. M.K., Gokulnath. C., and Devi. G.U. (2015) "Fuzzy Based Intrusion Detection Systems in MANET", *in Procedia Computer Science*, Vol. 50, 2015, pp 109-114. doi:10.1016/j.procs.2015.04.071

Basabaa. A., Sheltami. T., and Shakshuki. E. (2014) "Implementation of A3ACKs intrusion detection system under various mobility speeds", *in Procedia Computer Science 2014* 32, pp. 571–578, Elsevier. doi:10.1016/j.procs.2014.05.462

Batra. I., Hamatta. H.S.A., Malik. A., Mohammed Baz. M., Albogamy. F.R., Goyal. V., and Alshamrani. S.S. (2021) "LLSFIoT: Lightweight Logical Security Framework for Internet of Things", *in Wireless Communications and Mobile Computing,* Vol. 2021, 2021. doi:10.1155/2021/8526206

Boukerche. A., Turgut. B., Aydin. N., Ahmad. M.Z., Bölöni. L., and Turgut. D. (2011) "Routing protocols in ad hoc networks: A survey", *in Computer Networks* 55, 2011, pp. 3032–3080, Elsevier.doi:10.1016/j.comnet.2011.05.010

Casado, L.S., Carrión, R.M., Teodoro, P.G., and Verdejo, J.E.D. (2014) "Defenses against Packet-Dropping Attacks in Wireless Multihop Ad Hoc Networks", *in Khan, S., and Mauri, J.L. (eds) Security for Multihop Wireless Networks*, CRC Press, Boca Raton, FL. pp. 3-18

Chavan. A.A., Kurule. D.S., and Dere. P.U. (2016) "Performance analysis of AODV and DSDV routing protocol in MANET and modifications in AODV against black hole attack", *in Procedia Computer Science* 2016 79, pp. 835–844, Elsevier. doi:10.1016/j.procs.2016.03.108

Cheng. Y., Tang. Y., and Tsai. M. (2014) "LF-GFG: Location-Free Greedy-Face-Greedy Routing With Guaranteed Delivery and Lightweight Maintenance Cost in a Wireless Sensor Network With Changing Topology," *in IEEE Transactions on Wireless Communications,* Vol. 13(12), pp. 7025-7036, 2014. doi:10.1109/TWC.2014.2360844

Conti. M., Lal., Mohammadi. R., and Rawat. U. (2019) "Lightweight solutions to counter DDoS attacks in software defined networking", *in Wireless Networks* 25, pp. 2751–2768, 2019. doi:10.1007/s11276-019-01991-y

Casado, L.S., Carrión, R.M., Teodoro, P.G., and Verdejo, J.E.D. (2014) "Defenses against Packet-Dropping Attacks in Wireless Multihop Ad Hoc Networks", *in Khan, S., and Mauri, J.L. (eds) Security for Multihop Wireless Networks,* CRC Press, Boca Raton, FL. pp. 3-18

Dawoud, D.S., Gordon, L.R., Suliman A., and Raja, K. (2011) "Trust Establishment in Mobile Ad Hoc Networks: Key Management", *in Mobile Ad-Hoc Networks: Applications, Xin Wang, IntechOpen*. doi:10.5772/12866

Deb. N., Chakraborty. M., and Chaki. N. (2014b) 'CORIDS: a cluster-oriented reward-based intrusion detection system for wireless mesh networks', *in SECURITY AND COMMUNICATION NETWORKS*, 2014 7(3), pp. 532-543, Wiley. doi:10.1002/sec.750

Dhaka. A., Nandal. A., and Dhaka. R.S. (2015) "Gray and black hole attack identification using control packets in manets", *in Procedia Computer Science 2015* 54, pp. 83–91, Elsevier. doi:10.1016/j.procs.2015.06.01

Dorri. A. (2016) "An EDRI-based approach for detecting and eliminating cooperative black hole nodes in MANET", *in Wireless Networks 2016 23(6)*, pp. 1767–1778, Springer. doi:10.1007/s11276-016-1251-x

Dubey, S., and Saxena. P. (2016) "A review on collaborative decision technique for black-hole attack prevention in MANET", *in International Journal of Scientific & Engineering Research*, 7(2016), pp.230–236.

Funde. R., and Chandre. P. (2015) Dynamic Cluster Head Selection to Detect Gray Hole Attack using Intrusion Detection System in MANETs", *in Proceedings of the Sixth International Conference on Computer and Communication Technology 2015, Association for Computing Machinery*, pp. 73–77. doi:10.1145/2818567.2818581

Gaurav. A., and Singh. A.K. (2021) "Light weight approach for secure backbone construction for MANETs", *in Computer and Information Sciences* 33 2021, pp. 908–919. doi:10.1016/j.jksuci.2018.05.013

Gurung. S., and Chauhan. S. (2017) "A dynamic threshold based approach for mitigating black-hole attack in MANET", *in Wireless Networks 24*, 2016, pp. 2957-2971. doi:10.1007/s11276-017-1514-1

Hammamouche. A., Mawloud Omar. M., Djebari. N., and Tari. A. (2018) "Lightweight reputation-based approach against simple and cooperative black-hole

attacks for MANET", *in Journal of Information Security and Applications* 43 2018, pp. 12–20. doi:10.1016/j.jisa.2018.10.00

Hinge. R., and Dubey. J. (2016) "Opinion based trusted AODV routing protocol for MANET", *in Proceedings of the Second International Conference on Information and Communication Technology for Competitive Strategies.* 2016, 126, pp.1–5. doi:10.1145/2905055.2905342

Ibrahim, H.M., Omar, N.M., and William, E.K. (2015) "Detection and Removal of Gray, Black and Cooperative Black Hole Attacks in AODV Technique" *in International Journal of Advanced Computer Science and Applications (IJACSA),* 6(5). doi:10.14569/IJACSA.2015.060511

Jain, S., and Raghuwanshi, S.K. (2014) "Behavioural and node performance based Grayhole attack Detection and Amputation in AODV protocol," *in Proc International Conference on Advances in Engineering & Technology Research (ICAETR - 2014), Unnao, India*, pp. 1-5. doi:10.1109/ICAETR.2014.7012931

Jamshidi. M., Poor. S.S.A., Arghavani. A., Esnaashari. M., Shaltooki. A.A., and Meybodi. M.R. (2020) "A simple, lightweight, and precise algorithm to defend against replica node attacks in mobile wireless networks using neighboring information", *in Ad Hoc Networks,* Vol. 100, 2020. doi.org/10.1016/j.adhoc.2020.102081

Jayakumar, G., and Ganapathy,G. (2007) "Performance Comparison of Mobile Ad-hoc Network Routing Protocol.", *in IJCSNS International Journal of Computer Science and Network Security*, Vol.7 No.11

Jhaveri. R.H., and Patel. N.M. (2015) "A sequence number based bait detection scheme to thwart grayhole attack in mobile ad hoc networks", *in Wireless Networks* 21(8), 2015. pp.2781–2798, Springer. doi:10.1007/s11276-015-0945-9

Joseph. J.F.C., Das. A., Lee. B.S., and Seet. B.C.(2010) "Cross-layer based multiclass intrusion detection system for secure multicast communication of MANET in military networks", *in Computer Networks: The International Journal of Computer and Telecommunications Networking.* Vol. 54(7), 2010, pp. 1126–1141. doi:10.1016/j.comnet.2009.10.012

Kalkha. H., Satori. H., and Satori. K. (2019) "Preventing Black Hole Attack in Wireless Sensor Network Using HMM", *in Procedia Computer Science*, Vol. 148 2019, pp. 552-561. doi:10.1016/j.procs.2019.01.028

Kanthe, A.M., Simunic, D., and Prasad, R. (2012) "Comparison of AODV and DSR on-demand routing protocols in mobile ad hoc networks.", in *2012 1st International Conference on Emerging Technology Trends in Electronics, Communication & Networking*, pp. 1-5. doi:10.1109/ET2ECN.2012.6470118

Kaur. S., Kaur. S., and Sharma. C. (2013) "An Overview of Mobile Ad hoc Network: Application, Challenges and Comparison of Routing Protocols", *in IOSR Journal of Computer Engineering,* Vol. 11(5), pp. 7-11.

Khan, D., and Jamil, M. (2017) "Study of detecting and overcoming black-hole attacks in MANET: A review", *in Wireless Systems and Networks, International Symposium on IEEE*, 2017, pp. 1–4.

Khanna. N. (2016) "Avoidance and Mitigation of All Packet Drop Attacks in MANET using Enhanced AODV with Cryptography", *in International Journal of Computer Network and Information Security,* 2016,8(4), pp.37-43. doi:10.5815/ijcnis.2016.04.05

Khanna, N., and Sachdeva, M. (2019) "A comprehensive taxonomy of schemes to detect and mitigateblackhole attack and its variants in MANETs"., *in Computer Science Review*, 32 (2019), pp. 24–44. doi:/10.1016/j.cosrev.2019.03.001

Kumar. A., Saha. R., Alazab., M. and Kumar. G. (2020) "A Lightweight Signcryption Method for Perception Layer in Internet-of-Things*", in Journal of Information Security and Applications 55 2020.* doi:10.1016/j.jisa.2020.102662

Kumar. V., and Kumar. R. (2015) "An Adaptive Approach for Detection of Blackhole Attack in Mobile Ad hoc Network", *in Procedia Computer Science 48*, 2015, pp. 472–479.doi:10.1016/j.procs.2015.04.122

Lee. T.F., and Chen. W.Y. (2021) "Lightweight fog computing-based authentication protocols using physically unclonable functions for internet of medical things", *in Journal of Information Security and Applications* 59 2021. doi:10.1016/j.jisa.2021.102817

Liu. J., Zhao. H., Liu. C., and Jia. Q. (2021) "Privacy Data Security Policy of Medical Cloud Platform Based on Lightweight Algorithm Model", *in Scientific Programming,* Vol. 2021, Hindawi. doi.10.1155/2021/5543714

Mahamune. A.A., and Chandane. M.M. (2021) "An Efficient Trust-Based Routing Scheme Against Malicious Communication in MANET", *in International Journal of Wireless Information Networks*. Vol. 2021 28, pp.344–361. doi:10.1007/s10776-021-00523-w

Malekzadeh. M., Ghani. A.A.A., and Subramaniam. S. (2011) "Design and Implementation of a Lightweight Security Model to Prevent IEEE 802.11Wireless DoS Attacks", *in EURASIP Journal on Wireless Communications and Networking*, Vol. 2011, Hindawi. doi:10.1155/2011/105675

Marchang. N., and Datta. R. (2012) "Light-weight trust-based routing protocol for mobile ad hoc networks*", in IET Information Security 2012,* Vol. 6(2), pp. 77–83. doi:10.1049/iet-ifs.2010.0160

Martirosyan. A., and Boukerche. A. (2015) "LIP: an efficient lightweight iterative positioning algorithm for wireless sensor networks", *in Wireless Networks 22*, pp. 825–838, 2016. doi:10.1007/s11276-015-0982-4

Mitchell., R., and Chen. r. (2014) "A survey of intrusion detection in wireless network applications", *in Computer Communications*, 42 (2014) 1–23, Elsevier

Moudnia. H., Rouidib. M.E., Mouncifc. H., and Hadadia. B.E. (2019) "Black Hole attack Detection using Fuzzy based Intrusion Detection System in MANET", *in Procedia Computer Science* 151 (2019), pp. 1176–1181. doi:10.1016/j.procs.2019.04.168

Movahedi. Z., and Hosseini. Z. (2017) "A green trust-distortion resistant trust management scheme on mobile ad hoc networks", *in International Journal of Communication Systems, John Wiley & Sons, Ltd*., 2017 30(16). doi:10.1002/dac.3331

Mukhedkar. M.M., and Kolekar. U. (2019) "Trust-Based Secure Routing in Mobile Ad Hoc Network Using Hybrid Optimization Algorithm", *in The Computer Journal,* Vol. 62(10), 2019, pp. 1528–1545, Oxford Academic. doi:10.1093/comjnl/bxz061

Nadeem. A., and Howarth. M.P. (2013) "Protection of MANETs from a range of attacks using an intrusion detection and prevention system", *in Telecommunication Systems,* Vol. 52, pp. 2047–2058 (2013). doi:10.1007/s11235-011-9484

Nadeem. A., and Howarth. M.P. (2014) "An intrusion detection & adaptive response mechanism for MANETs*", in Ad Hoc Networks*, Vol. 13 B, 2014, pp. 368-380. doi:10.1016/j.adhoc.2013.08.017

Nand. P., Sharma. S.C., and Astya. R. (2010) "Traffic Load based Performance Analysis of DSR, STAR & AODV Adhoc Routing Protocol", *in International Journal of Advanced Computer Science and Applications,* Vol. 1(4), 2010, pp. 58-62. doi:10.14569/IJACSA.2010.010410

Olmos. M.D.S., Orallo. E.H., Cano. J.C., Calafate. C.T., and Manzoni. P. (2012) "Accurate detection of black holes in MANETs using collaborative bayesian watchdogs", *2012 IFIP Wireless Days*, 2012, pp. 1-6. doi:10.1109/WD.2012.6402811

Ourouss. K., Naja. N., and Jamali. A. (2020) "Defending Against Smart Grayhole Attack Within MANETs: A Reputation-Based Ant Colony Optimization Approach for Secure Route Discovery in DSR Protocol", *in Wireless Personal Communications*, 116, 2021, pp. 207–226, Springer. doi:10.1007/s11277-020-07711-6

Pandey. S., and Singh. V. (2020) "Black-hole Attack Detection Using Machine Learning Approach on MANET," *in 2020 International Conference on Electronics and Sustainable Communication Systems (ICESC),* 2020, pp. 797-802. doi:10.1109/ICESC48915.2020.9155770

Panos, C., Ntantogian, C., Malliaros, S., and Xenakis, C. (2016) "Analyzing, Quantifying, and Detecting the Black-hole attack in Infrastructure-less Networks*", in Computer Networks 2016*. Vol. 113, pp.94-110. doi:10.1016/j.comnet.2016.12.006

Patel. A.D., and Chawd. K. (2015). "Dual Security Against Grayhole Attack in MANETs", *In: Jain. L., Patnaik. S., and Ichalkaranje. N. (Eds) Intelligent Computing, Communication and Devices. Advances in Intelligent Systems and Computing*, Vol. 309. Springer. doi:10.1007/978-81-322-2009-1_4

Pathan. M.S., Jingsha He. J., Zhu. N., Zardari. Z.A., and Memon. M.Q. (2019) "An Efficient Scheme for Detection and Prevention of Black Hole Attacks in AODV-Based MANETs*", in (IJACSA) International Journal of Advanced Computer Science and Applications,* Vol. 10(1) 2019, pp. 243-251. doi:10.14569/IJACSA.2019.0100132

Perking, P.E., Royer, E.B., and Das, S. (2003) "Ad-hoc on-demand distance vector routing," No. RFC 3561, 2003

Poongodi, M., and Bose. S. (2015) "Detection and prevention system towards the truth of convergence on decision using aumann agreement theorem", *in*

Procedia Computer Science 50 (2015) pp. 244–251, Elsevier. doi:10.1016/j.procs.2015.04.053

Poongodi, T., and Karthikeyan, M. (2016) "Localized Secure Routing Architecture Against Cooperative Black Hole Attack in Mobile Ad Hoc Networks", in Wireless Personal Communication 90, pp. 1039–1050, 2016. doi:10.1007/s11277-016-3318-5

Rana. A., Rana. V., and Gupta. S. (2015) "EMAODV: Technique to prevent collaborative attacks in MANETs", in Procedia Computer Science 2015 70, pp.137–145, Elsevier. doi:10.1016/j.procs.2015.10.060

Rangaraj. J., and Anitha. M, (2017) "Performance Analysis Of Proactive And Reactive Protocol Under Different Mobility Models For Manet", in International conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud)*(I-SMAC)*, 2017, pp. 637-643. doi:10.1109/I-SMAC.2017.8058257

Reddy. B.P., Reddy. B.B., and Dhananjaya B. (2021), "The AODV routing protocol with built-in security to counter black-hole attack in MANET" in Materials Today: Proceedings, Elsevier, 50(5), 2021, pp. 1152-1158. doi:10.1016/j.matpr.2021.08.039

Reddy. M.C.K., Sujana. A., Sujitha. A., and Rudroj. K. (2018) "Comparing the Throughput and Delay of Proactive and Reactive Routing Protocols in Mobile Ad-hoc Networks", in Proceedings of the Second International Conference on Inventive Systems and Control (ICISC 2018), 2018, pp. 1278-1283. doi:10.1109/ICISC.2018.8399011

Rmayti. M., Khatoun. R., Begriche. Y., Khoukhi. L., and Gaiti. D. (2017) "A stochastic approach for packet dropping attacks detection in mobile Ad hoc networks", in Computer Networks, Vol. 121, 2017, pp. 53-64. doi:10.1016/j.comnet.2017.04.027

Salunke. A., and Ambawade. D. (2015) "Dynamic Sequence Number Thresholding Protocol for Detection of Blackhole Attack in Wireless Sensor Network" in 2015 International Conference on Communication, Information & Computing Technology (ICCICT), 2015, pp. 1-4. doi:10.1109/ICCICT.2015.7045745

Santos. M.L.B.A., Carneiro. J.C., Franco. A.M.R., Teixeira. F.A., Henriques. M.A.A., and Oliveira. L.B. (2020) "FLAT: Federated Lightweight Authentication for the Internet of Things", in Ad Hoc Networks 2020. doi:10.1016/j.adhoc.2020.102253

Schellenberg. R.S., Wang. N., and Wright. D. (2020), "Performance Evaluation and Analysis of Proactive and Reactive MANET Protocols at Varied Speeds", in 2020 10th Annual Computing and Communication Workshop and Conference (CCWC), IEEE, 2020, pp. 0981-0985.doi:10.1109/CCWC47524.2020.9031233

Semary, A.M.E., and Diab, H. (2019) "BP-AODV: Blackhole Protected AODV Routing Protocol for MANETs Based on Chaotic Map," *in IEEE Access*, Vol. 7, pp. 95197-95211. doi:10.1109/ACCESS.2019.2928804

Sen.J., Chandra. M. G., Harihara. S. G., Reddy. H., and Balamuralidhar. P. (2007) "A mechanism for detection of gray hole attack in mobile Ad Hoc networks", *in 2007 6th International Conference on Information, Communications & Signal Processing*, 2007, pp.1-5. doi:10.1109/ICICS.2007.4449664

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

Shahzamal, M.D. (2018) "Lightweight Mobile Ad-hoc Network Routing Protocols for Smartphones", *in Networking and Internet Architecture, Multi-agent Systems, Cornell University Library*. doi:10.48550/arXiv.1804.0213

Shukla, M., Joshi. B.K., and Singh. U. (2021) "Mitigate Wormhole Attack and Blackhole Attack Using Elliptic Curve Cryptography in MANET", *in Wireless Personal Communications 121,* pp. 503–526, 2021. doi:10.1007/s11277-021-08647-1

Singh. M., and Singh. P. (2016) "Black Hole Attack Detection in MANET Using Mobile Trust Points with Clustering", *In: Unal. A., Nayak. M., Mishra. D.K., Singh. D., and Joshi. A. (eds) Smart Trends in Information Technology and Computer Communications. SmartCom 2016. Communications in Computer and Information Science*, Vol. 628. Springer. doi:10.1007/978-981-10-3433-6_68

Singh, O., Singh, J., and Singh, R. (2018) "Multi-level trust based intelligence intrusion detection system to detect the malicious nodes using elliptic curve cryptography in MANET", *in Cluster Computing 21*, pp. 51–63, 2018. doi:10.1007/s10586-017-0927-z

Shahzamal, M.D. (2018) "Lightweight Mobile Ad-hoc Network Routing Protocols for Smartphones", *in Networking and Internet Architecture, Multi-agent Systems, Cornell University Library*. doi:10.48550/arXiv.1804.02139

Shakshuki. E.M., Kang. N., and Sheltami. T.R. (2013) "EAACK: A Secure intrusion-detection system for MANETs", *in IEEE Transactions on Industrial Electronics.* 2013, 60 (3), pp. 1089–1098, IEEE. doi:10.1109/TIE.2012.2196010

Sharma, A., and Kumar, R. (2016) "Performance Comparison and Detailed Study of AODV, DSDV, DSR, TORA and OLSR Routing Protocols in Ad Hoc Networks", *in: 2016 Fourth International Conference on Parallel, Distributed and Grid Computing (PDGC),* pp. 732-736, IEEE. doi:10.1109/PDGC.2016.7913218

Sharma. B. (2015) "A Distributed Cooperative Approach to Detect Gray Hole Attack in MANETs", *in Proceedings of the Third International Symposium on Women in Computing and Informatics*, pp. 560–563. doi:10.1145/2791405.2791433

Shi. F., Liu. W., Jin. D., and Song. J. (2014) "A cluster-based countermeasure against black-hole attacks in MANETs", *in Telecommunication Systems* 57, 2014 pp. 119–136. doi:10.1007/s11235-013-9788-9

Shrestha. S., Baidya. R., Giri. B., and Thapa. A. (2020) "Securing Blackhole Attacks in MANETs using Modified Sequence Number in AODV Routing Protocol", *in 2020 8th International Electrical Engineering Congress (iEECON),* 2020, pp. 1-4. doi:10.1109/iEECON48109.2020.229555

Song. C.H., Jianyu. Z., and Lee. H. W. J. (2008) "A novel NP-based security scheme for AODV routing protocol", *in Journal of Discrete Mathematical Sciences and Cryptography, 2008* 11:2, pp. 131-145. doi:10.1080/09720529.2008.10698172

Song. S., Choi. H.K., and Kim. J.Y. (2009) "A Secure and Lightweight Approach for Routing Optimization inMobile IPv6", *in EURASIP Journal on Wireless Communications and Networking,* Vol. 2009. doi:10.1155/2009/957690

Sooriyaarachchi. S.J. (2016) '*Routing and Control Mechanisms for Dense Mobile Adhoc Networks'*. PhD thesis. University of Moratuwa, Sri Lanka. url:http://dl.lib.uom.lk/handle/123/15847

Subba. B., Biswas. S., and Karmakar. S. (2016) "Intrusion detection in Mobile Ad-hoc Networks: Bayesian game formulation", *in Engineering Science and Technology, an International Journal*, Vol. 19(2), 2016, pp. 782-799. doi:10.1016/j.jestch.2015.11.001

Subramaniyan, S., Johnson, W., and Subramaniyan, K. (2014) "A distributed framework for detecting selfish nodes in MANET using Record- and Trust-Based Detection (RTBD) technique", *in EURASIP Journal on Wireless Communications and Networking*, 205 (2014). doi:10.1186/1687-1499-2014-205

Sun. H.M., Chen. C.H., and Ku. Y.F. (2012) 'A novel acknowledgment-based approach against collude attacks in MANET", *in Expert Systems with Applications: An International Journal*, 2012 39(9), pp. 7968–7975, Elsevier. doi:10.1016/j.eswa.2012.01.118

Suraj. R., Tapaswi. S., Yousef. S., Pattanaik, K.K., and Cole. M. (2015) "Mobility prediction in mobile ad hoc networks using a lightweight genetic algorithm", *in Wireless Networks* 22, pp. 1797–1806, 2015. doi:10.1007/s11276-015-1059-0

Teodoro, P.G., Casado, L.S., and Fernández, G.M. (2014) "Taxonomy and Holistic Detection of Security Attacks in MANETs", *in Khan, S., and Mauri, J.L. (eds) Security for Multihop Wireless Networks*, CRC Press, Boca Raton, FL. pp. 377-400

Tran. T.M.C., Scheuermann. B., and Mauve. M. (2009) "Lightweight detection of node presence in MANETs", *in Ad Hoc Networks 7 (2009),* pp. 1386–1399, Elsevier. doi:10.1016/j.adhoc.2009.02.002

Usha. G., Babu. M.R., and Kumar. S.S. (2016) "Dynamic anomaly detection using cross layer security in MANET", *in Computers & Electrical Engineering*, Vol. 59, 2016, pp. 231-241. doi:10.1016/j.compeleceng.2016.12.002

Vijayakumar. A., Selvamani. K., and Arya. P.K. (2015) "Reputed Packet Delivery Using Efficient Audit Misbehaviour Detection and Monitoring Method in Mobile Ad Hoc Networks", *in Procedia Computer Science,* Vol. 48,2015, pp. 489-496. doi:10.1016/j.procs.2015.04.124

Wang. J., Liu. Y., Niu. S., and Song. H. (2021) "Lightweight blockchain assisted secure routing of swarm UAS networking", *in Computer Communications* 165 2021, pp. 131–140. doi:10.1016/j.comcom.2020.11.008

Wang. Z., Chen. Y., and Li. C. (2014) "PSR: A Lightweight Proactive Source Routing Protocol For Mobile Ad Hoc Networks," *in IEEE Transactions on Vehicular Technology,* Vol. 63(2), pp. 859-868, 2014. doi:10.1109/TVT.2013.2279111

Wen. Y., Yang. Y., Wang. S., Li. L., and Luo. M. (2020) "A New Certificateless Aggregate Signature Scheme for Wireless Sensor Networks", *in Wang. G., Chen, B., Li. W., Pietro D.R., Yan. X., and Han. H. (Eds) Security, Privacy, and Anonymity in*

Computation, Communication, and Storage. SpaCCS 2020. Lecture Notes in Computer Science, Vol. 12382. Springer. doi:10.1007/978-3-030-68851-6_23

Wool. A (2005) "Lightweight Key Management for IEEE 802.11Wireless LANs with Key Refresh and Host Revocation", *in Wireless Networks 11*, 2005, pp. 677–686, Springer. doi:10.1007/s11276-005-3522-9

Xia. H., Yu. J., Tian. C., Pan. Z., and Sha. E. (2016) "Light-weight trust-enhanced on-demand multi-path routing in mobile ad hoc networks", *in Journal of Network and Computer Applications,* Vol. 62, 2015, pp. 112-127. doi:10.1016/j.jnca.2015.12.005

Zhang. P., Lin. C., Jiang. Y., Fan. Y., and Shen. X.S. (2013) A Lightweight Encryption Scheme for Network-Coded Mobile Ad Hoc Networks", *in IEEE Transactions on Parallel and Distributed Systems*, Vol. 25(9), pp. 2211-2221, 2014. doi:10.1109/TPDS.2013.161

Zhang. Z., Boukerche. A., and Ramadan. H. (2012) "Design of a lightweight authentication scheme for IEEE 802.11p vehicular networks", *in Ad Hoc Networks 10 (2012),* pp. 243–252, Elsevier. doi:10.1016/j.adhoc.2010.07.018