Indonesian Journal of Electrical Engineering and Computer Science
Vol. 21, No. 2, February 2021, pp. 1193~1200
ISSN: 2502-4752, DOI: 10.11591/ijeecs.v21.i2.pp1193-1200

An end to end key establishment scheme for detecting black hole attacks in mobile ad hoc networks

Baban Ahmed Mahmood[1], Aso Ahmed Majeed[2], Ahmed Chalak Shakir[3]
[1,3]Network Department, College of Computer Science and Information Technology, Kirkuk University, Iraq
[2]Department of Parasitology, College of Veterinary Medicine, Kirkuk University, Iraq

Article Info

Article history:

Received Jul 10, 2020
Revised Sep 7, 2020
Accepted Sep 27, 2020

Keywords:

Black hole attacks
Reactive routing
Routing in MANETs
Security of routing in MANETs

ABSTRACT

The wireless technology is in consistent and rapid development in this century such that it produces fast data rate and strong connectivity. Mobile ad hoc network (MANET) is an independent network wherein nodes function as both host and router. Routing protocols in MANET are prone to different attacks. Malicious nodes usually interfere the process of establishing routes and make it hard to build a valid route. In the literature, different mechanisms proposed to prohibit black hole attacks in which an adversary node blindly drops data packets. In this paper, a study is fulfilled of the advantages and disadvantages of some of the protocols presented in the literature and a novel method proposed that detects black hole attacks. A thorough, precise, and theoretical analysis is presented to show how the proposed method can prevent malicious nodes from impersonating benign nodes. A theoretical compareison conducted between the proposed method and some of the other methods presented in the literature. The comparison shows that the attacks exist on these protocols are detected and prevented by the proposed protocol.

Corresponding Author:

Baban Ahmed Mahmood
Network Department
College of Computer Science and Information Technology
Kirkuk University
Baghdad Street, Kirkuk, Iraq
Email: baban.mahmoodjaf@gmail.com

1. INTRODUCTION

The nodes in MANET get through with each other to set up a network in an uncontrolled area without any pivotal organization such as Base Stations (BS) [1, 2]. Through the communication links, the nodes cooperatively send packets acting as routers [3-6]. MANETs can be applied in different scenarios within uncontrolled fields such as military, animal habitats, natural disasters, rescue operations, etc., where building communication infrastructure is not possible [7-11]. Routing is divided into two main phases: establishing route phase and data packets dispatching phase. Phase one is responsible of discovering a legitimate route between source and target nodes whereas second phase is concerned about forwarding the data packets through the established route. In secure routing protocols, participating nodes can exchange both data and control information regardless of the availability of vicious nodes whose purpose is to deteriorate the routing protocol's functionality [12]. The authors in [13] present a survey of different mechanisms that provide secure routing features for MANET. MANET's main characteristics like dynamic topology, open medium, and distributed nature of nodes' operation make it highly vulnerable. Also, Routing is an essential part of the network's security wherein malicious nodes can claim they have valid routes to destination nodes. Black hole is a possible attack on routing which is a threat that adversely affects data forwarding process [2,

14, 15]. Passive and active attacks are two fundamental types of attacks out there targeting routing protocols [16]. The routing operation in passive attacks is not disrupted by adversarial nodes while adversarial nodes in active attack disrupt regular operations of the network operations and execute violations. The disruption and violation may occur at different levels including both data forwarding and route discovery levels [8, 17]

An attacker may disrupt the network operation by offering a path that is shorter than the path provided by a genuine node [4, 18, 19]. This type of attack is done by changing some of the control information or metrics of routing. Impersonation is another type of attack wherein malicious node use identity belonging to other nodes to initiate attacks [20-22]. There are different security mechanisms to address the malicious or adversarial nodes [23]:

a) Preventive Mechanism This mechanism works as a defense technique by applying encryption and authentication schemes. In these schemes, symmetric key and asymmetric key cryptography are used.
b) Reactive Mechanism Misuse and anomalies are detected in this mechanism. In the anomaly detection case, statistically, the normal behavior of the participating nodes is calculated by collecting useful information from genuine nodes' behavior. Then, nodes' anomalous behaviors are detected by analyzing the calculated statistical tests.

1) Black hole

Black hole is an adversary node that is blindly replying to route request (RREQ) messages received from neighboring nodes. This attacker claims it has a valid and fresh path to the target. Then it takes in each and every data packet directed to that target node. It is hard to detect black hole nodes that use a better sequence number especially if the network's sequence number is close to the one utilized by the attacker [3, 15, 24].

Figure 1 shows how black hole attack can disrupt the routing process in MANET. The source node *S* intends to send data packets to the target *D*; hence, it has to discover a route to *D*. Under the AODV [25] protocol which is presented later in 3.1.1, *S* floods a RREQ control packet to the ad hoc network aiming to establish a route to node *D*. In the normal operation of AODV, benign and vicious nodes receive the request. However, the attacker (*B*) replies with fake information such that the source node receives a reply whose sequence number is high. Also, the destination and the intermediate nodes (e.g. 2 and 4) that have valid routes return route reply (RREP) packets to the source *S* with their actual sequence numbers which are usually lower than the black hole node's sequence number. Thus, *S* picks *B's* route reply to build a route to *D*. After it controls the routing process, *B* discards every data packet from being forwarded to node *D* [4]. In case there is no security technique, node *S* cannot determine whether the data packets are delivered to *D*.

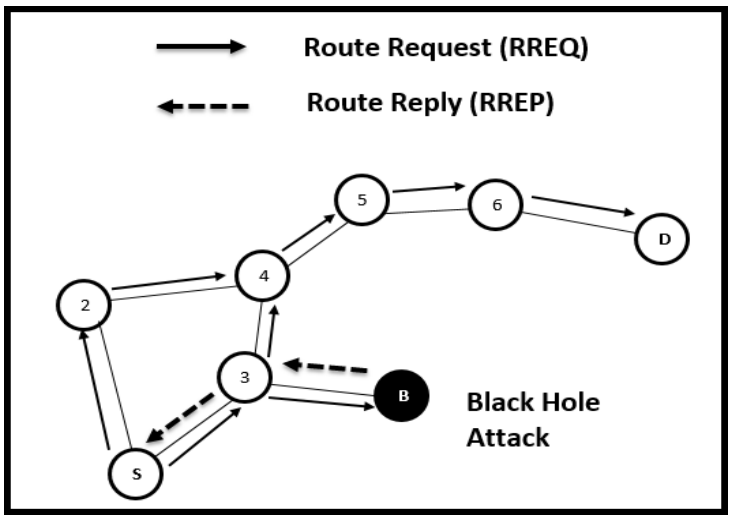

Figure 1. Black hole attack during route request flooding [4].

2) Basic route discovery

Under reactive routing protocols like AODV, a route to a destination *D* is discovered when a source *S* attempts to forward packets to *D*. *S* dispatches an announcement requesting all its neighbor nodes for a path over which packets travels to *D*. When they receive the request, intermediate nodes reply to the source in

case they have credible paths to the destination. If they don't, the intermediate nodes rebroadcast the request to all their neighboring nodes. This rebroadcasting stops if *S* locates a legitimate route to the *D*. The main criteria to pick a reply among several responses is to search for the highest sequence number.

3) Paper objective and motivation

Some of the protocols are prone to black hole attacks targeting the route establishment phase. An analysis of these these attacks is performed and a secure method for routing in MANET that basically depends on end to end key establishment scheme is produced. In the proposed method, malicious nodes are prevented from disrupting the process of route establishment. *Hence, the primary contribution is first, designing a secure method that detects black hole attacks. Second, detecting the attacks on the protocols that are presented in the literature which are prone to this type of attack.*

The rest of the paper is organized as follows: In Section 2, we examine some of the recent protocols that claim to reveal black hole attacks. In Section 3, the details of the proposed protocol design is presented. Section 4 presents a theoretical analysis of the proposed method. In Section 5, the drawbacks of some of the protocols presented in Section 2 are shown as well as the way these attacks are detected and prevented by the proposed protocol is explained. In Section 6, a conclusion of the paper is presented.

2. RELATED WORK

A concise explanation of the basic idea concerning some of the recently proposed black hole attack detection schemes is presented here. These methods are proposed to work on on-demand routing protocols that are independent on network topology to establish routes. Yaseena and Aldwairia in [2] proposed an enhanced AODV to avoid black hole nodes in MANET. They used a reputation table to block a black hole or a misbehaving node from disrupting route creation. This protocol works in three main phases namely, accumulating reputation values, calculating these values, and picking the best route. Observations, reputation values, are collected by making use of AODV's watchdog's approaches. These observations rely upon observations of neighbors that are done individually. Later, the reputation values are broadcast to the entire network.

Kalkha et al. in [15] presented a protocol that makes use of black hole prevention technique to identify adversarial nodes using Hidden Marcov Model. Their method works in two modules namely, detection and decision-making. In the detection module, an analysis is done for the shortest routes found between source and destination pair. This analysis is performed using Hidden Marcov Model such that the most possible attacker is found. In the decision module, the shortest routes that contain untrusted nodes are eliminated from the routing tables.

Singh and Sharma in [1] proposed a mechanism that depends on the promiscuous mode of the node in which, nodes are allowed to read and intercept packets. When a source node *S* intends to forward data packets to a target node *T*, it broadcasts a request to locate a route from the route replies (RREP) it receives as a response to the request. When the RREP is originated from a transitional, intermediate, node *N*, the preceding node *P* of *N* changes its mode to a promiscuous mode which then sends a hello message to the *T* via *N*. If *T* receives the message, it means that *N* is benign and the route is free from harm. Otherwise, this intermediate, *N*, node is considered an adversary and an alarm is broadcast to the network by the preceding node P warning them about this malicious node.

Arathy and Sminesh in [26] proposed an algorithm which detects multiple black hole attack (D-MBH). In addition to multiple attacks, using extra route request, this algorithm prevents single black hole attack from disrupting routing creation process. Without the destination address, the algorithm computes a threshold average destination sequence number (ADSN), maintains a list that contains black hole nodes that collaboratively establish a non-valid route. It is worth mentioning that this protocol uses extra RREQ control packet and maintains additional tables of collaborative black hole nodes. This extra control information obviously increases overhead in addition to increasing the response time. Also, it limits scalability as depicted in Table 1.

Jain et al. in [27] presented a fuzzy-based trust to enhance security in MANETs to prevent black hole attacks. A relational fuzzy binary weighted model is used to mitigate the distractions caused by adversarial nodes against AODV routing protocol. The trust computation is performed in a direct way on fuzzy approaches to identify malicious nodes.

Sharma et al. in [3] proposed a method that uses two solutions for black hole attack blockage. The first solution is to discover multiple routes (more than two routes) by flooding route requests to reach the destination. The source ***S*** then sends different ping messages via the multiple routes found in the first place to the destination node ***D***. Each message has its own identifier (ID) and sequence number. Any intermediate node, both benign and malicious, may acknowledge or reply to this ping packet when they have a path to the

destination. Different acknowledgments are collected by the source which it then uses them to differentiate between malicious nodes and honest nodes. It is explained in Section 5 how this solution has drawbacks and limitations because MANETs come with different scenarios. The second solution makes advantage of packet sequence number which was included in the packet header by using two extra tables in each node. The first table contains the last packet's sequence number that was sent to each node while the other table contains the sequence number which was sent from other nodes. Destination or intermediate nodes use these two tables when they reply to route requests. They must imbed the last packet's sequence number sent by the source nodes. The source node then compares this imbedded sequence number with the second table's sequence numbers and if a match is found, the replier is considered benign; otherwise the replier is considered adversary node and a warning message is broadcast to the entire network.

Junhai Luo et al. in. [14] proposed an authentication mechanism wherein black hole attacks are prevented. The authentication is based on message authentication code, pseudo random function, and hash function that are applied on AODV. When the sender, source, receives the route reply, it applies the authentication scheme proposed to make a proper decision. However, intermediate nodes' role is only forwarding data packets, in other words, no verification is performed by intermediate nodes. The destination node performs four different steps to authenticate the control packet including symmetric cryptosystem, finding decrypted message, calculating message authentication code (MAC), and calculating a reasonable time stamp (TS). If all these verifications are achieved successfully, the route is valid and the sender begins to forward packets; otherwise, the sender performs another route discovery and warns the network about the malevolent node in the network.

3. PROPOSED DESIGN

The main idea of the proposed method is presented in this Section under which, a secure route is discovered connecting a source to a destination node. Also, the proposed protocol detects black hole attacks on various MANET's routing protocols. This proposed algorithm can be applied to any reactive topology based routing protocol (e.g., AODV) that establishes routes prior to forwarding data packets. In this paper, we use the concepts of AODV to show the workflow of the proposed protocol. In the following subsections, an explaination of the above mentioned points is given.

3.1. Basic idea of the protocol

Routing protocols in MANET are prone to several attacks like black hole attacks, blackmail attacks, hidden channel attacks, etc. [28-30]. The main focus here is to prohibit the black hole attacks. In the following, a thorough explanation of the proposed method is given.

3.1.1. End to end key establishment

Following the route discovery phase as explained in Section 1.2., once a route reply arrives at the source node, a route to the destination is established. To verify the validity of the route built, the source ***S*** sends a key establishment control packet through the established route to the destination *D* as shown in Figure 2. This control packet consists of a Nonce (*N1*) concatenated with a Random Secret Key (*RSKs*) generated by the source node. The packet is then encrypted using the public key (*PKd*) of the destination node and sent to the destination node. We assume that the source and the destination know the public key of each other.

When *D* receives the control packet, it decrypts the packet using its private key and gets both the *N1* and the *RSKs*. The destination generates a Random Secret Key (*RSKd*) and calculates the shared key (*Ksd*). Ksd is calculated by XORing the two random secret keys *RSKs* and *RSKd* respectively. After finding the shared secret key, *D* sends a control reply packet to *S*. The reply packet consists of both the received Nonce *N1* and *D's* Random Secret Key *RSKd*. This packet is encrypted using the Random Secret Key of the source node *RSKs*. When the reply is received from *D* by *S*, the source checks the Nonce and gets *D's* Random Secret Key *RSKd* which it uses to calculate the shared key *Ksd*. To guarantee that *S* and *D* now have the same shared secret key, *S* sends a probe packet to *D*. The probe packet is a new Nonce *N2* which is encrypted using *Ksd*. Once *D* receives that probe packet, it decrypts the packet, obtains *N2*, append its *RSKd*, encrypts it again using the shared key, and sends the newly encrypted packet to S which in turn verifies that it is from *D* and *N2* and *RSKd* are correct. After that both *S* and *D* delete their Random Secret Keys. Then *S* starts forwarding data packets through the established route. Proper description of the proposed protocol for route validation and data forwarding is given in Figure 3

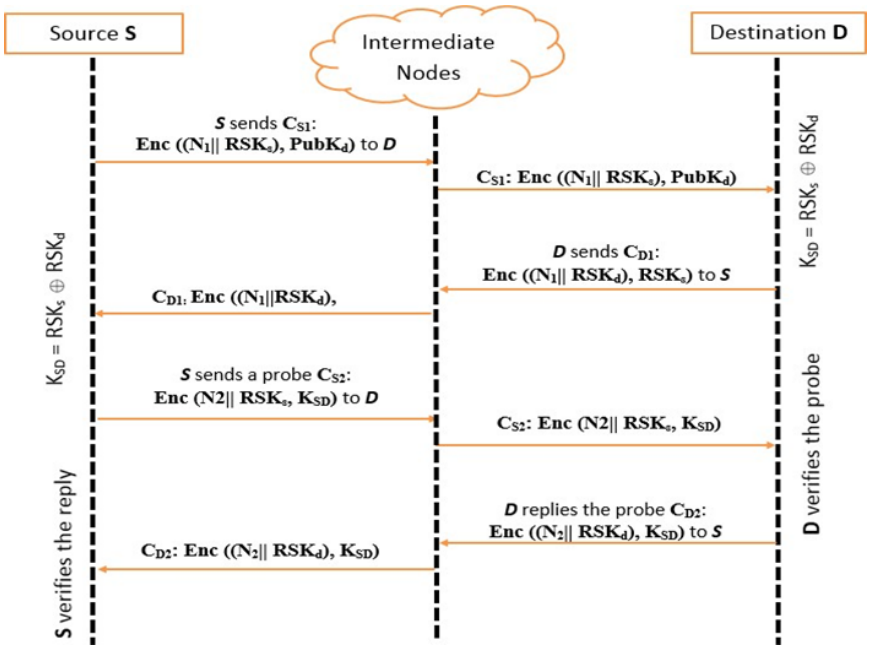

Figure 2. End to end key establishment

When a source node S wants to send a data packet to a destination node D:

Let *L* be the list of neighbors of S;

If *L* is empty, **Then**

Drop the data packet /* No neighbors*/

Else

Perform route discovery process similar to AODV

If (Verify_Route_Validity()) is True, **Then**

Start data forwarding

Else

Put the node originating RREP into a black list

Broadcast the black list to the entire network.

Figure 3. Data forwarding and route validation process

4. ANALYSIS

In this section, a thorough examine of how the proposed method prohibits the black hole attacks that exist in some of the protocols mentioned in Section 2 is presented. Some of the issues taken into consideration in designing these protocols are: security, scalability, reducing control overhead, load balancing, fault-tolerance, robustness, and shrinking complexity. Counting on how well the discussed protocols treat these issues, we rate the protocols as *Low*, *Medium*, and *High* concerning the above mentioned factors as shown in Table 1. Next, how black hole attacks are detected by the proposed method is presented then an explanation and detection of some of the attacks on the protocols presented in the literature are demonstrated.

Table 1. Comparison of the protocols presented in the literature with respect to different features

Protocol	Scalability	Overhead	Security	Mechanism
Reference [3]	Medium	High	High	Multiple Routes
Reference [1]	High	Medium	Low	Promiscuous Mode
Reference [26]	Medium	High	Medium	Threshold Sequence Number
Reference [2]	High	Medium	Medium	Watchdog and Reputation Table
Reference [14]	Medium	High	Medium	Authentication
Reference [15]	Medium	High	Medium	Markov Model

4.1. Black hole detection by the proposed protocol

This Section shows how the proposed protocol can detect any possible black hole attack describing different scenarios related to route breakage or attack. The handshaking process presented in Section 3.1.1 helps in detecting a black hole attack if there is any. As mentioned in Section 3.1.1, the key establishment process starts after receiving a route reply which could be from an intermediate node IN. This intermediate node could be either a benign node or a malicious node. The Malicious node has no fresh route to the target, but it claims it has one. To detect the credibility of this intermediate node, the source S launches the key establishment process via the route that was built after the intermediate node had replied. If S receives a response from the destination, it means that IN is benign. If not, then IN is a black hole and S inserts this node into its black list table. It is possible that the.

Route between S and D has broken. To distinguish between these two cases, a route error message is used. When a node in an established route goes down or when it is no more connected to the route, the upstream node of the break broadcasts a route breakage notification message. If receives this error message before receiving the response from the destination node D, it needs to issue another route discovery and perform black hole detection to the newly established route. It is also possible that the link between the S and IN has broken. In this case, S receives a route error message issued by an intermediate node upstream to IN, hence S cannot verify the honesty of IN because the verification signal could not reach IN. When a black hole is noticed, a message is broadcast by *S* to the network in which *S* announces that node *IN* is malicious and accordingly, every node inserts *IN* into its black list. This process alleviates future black hole by preventing formerly detected malicious nodes from being involved in the routing path.

5. DISCUSSION

Here, a precise discussion of how the proposed method detects and prevents the attacks by the vicious nodes on three of the protocols mentioned in the literature is presented and the way these attacks affect the routing is discussed.

5.1. Attack on the protocol in reference [1].

The verification in [1] is not encrypted, as well, the promiscuous mode of the node gives the black hole node a chance to pass the hello packet to the destination as well as impersonate the destination node. As a result, all the data packets are dropped because the source considers this as a valid route. However, it is important to notice that in the proposed method the verification packet is not in plain text. This prevents the black hole node to impersonate the destination. This is because it does not know this is a verification packet and it may drop it which means that this route cannot be verified and as a result the attack is detected. Hence, the proposed design detects black hole nodes that use impersonation techniques.

5.2. Attack on the protocol in reference [2].

One possible drawback of the protocol presented in [2] is that when there is only one path, the protocol will choose it regardless of its reputation value. The selected path could have malicious node that drops the data packets which disrupts the data forwarding process. The proposed protocol detects such attacks because a secured verification control message is used to check the authenticity of the malicious node in the path which easily prevents the adversary node from disrupting the routing establishment process.

5.3. Attack on the protocol in reference [3].

The solutions proposed in [3] is not feasible when the network is sparse, in other words, requiring three routes at least imposes the network to be dense such that multiple routes can be established. This density feature as well as multiple extra tables used in their second solution limits the scalability of the network; this is depicted in Table 1. Even-though, in sparse networks, this protocol may not find three different routes which deteriorates its normal operation and as a result, a secure route is not established. Also, in case of single route, which may contain malicious nodes, a fake route can be established. This shortcoming and other problems in this method can be solved using the security features provided by the proposed method where verified messages are used to establish routes making only benign nodes to participate in building routes.

6. CONCLUSION

In this paper, we produced a secure and novel algorithm that notices and prohibits black hole attacks on MANETs. This proposed protocol counts on end-to-end key establishment which depends on public key cryptography. The proposed security scheme is general such that it can be applied to any on demand routing

protocol. A detailed analysis and discussion of the attacks currently exist on routing protocols are provided. The detection analysis showed that the proposed method notices these attacks as well as blocks them from disrupting the data forwarding and route establishment process. Hence, this proposed scheme prevents most of the black hole attacks attempted by malicious nodes.

REFERENCES

[1] P. Singh and G. Sharma, "An efficient prevention of black hole problem in aodv routing protocol in manet," *in Proceedings of IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)*, pp. 902-906, 2012.

[2] Q. M. Yaseen and M. Aldwairi, "An enhanced aodv protocol for avoiding black holes in manet," *Procedia Computer Science*, vol. 134, pp. 371-376, 2018.

[3] N. Sharma and A. Sharma, "The Black-Hole node attack in Manet," *in 2012 second international conference on Advanced Computing & Communication Technologies. IEEE*, pp. 546-550, 2012.

[4] H. Moudni, M. Er-Rouidi, H. Mouncif, and B. El Hadadi, "Fuzzy logic-based intrusion detection system against black hole attack in mobile ad hoc networks," *International Journal of Communication Networks and Information Security*, vol. 10, no. 2, pp. 366-373, 2018.

[5] H. Li and M. Singhal, "An anchor-based routing protocol with cell id management system for ad hoc networks," *in Proceedings of International Conference on Computer Communications and Networks*, pp. 215-222, 2005.

[6] B. A. Mahmood and D. Manivannan, "Position based and hybrid routing protocols for mobile ad hoc networks: a survey," *Wireless Personal Communications*, vol. 83, no. 2, pp. 1009-1033, 2015.

[7] S. Jain, A. Shastri, and B. K. Chaurasia, "Analysis and feasibility of reactive routing protocols with malicious nodes in manets," *in Proceedings of International Conference on Communication Systems and Network Technologies (CSNT)*, pp. 356-360, 2013.

[8] G. Liu, H. Dong, Z. Yan, X. Zhou, and S. Shimizu, "B4SDC: A blockchain system for security data collection in manets," *IEEE Transactions on Big Data*, vol. 14. no. 8. pp. 1-14, 2015.

[9] V. N. Talooki, H. Marques, and J. Rodriguez, "Energy efficient dynamic manet on-demand (e2dymo) routing protocol," *in Proceedings of International Symposium and Workshops on a World of Wireless, Mobile and Multimedia Networks (WoWMoM)*, pp. 1-5, 2013.

[10] H. Shen and L. Zhao, "Alert: An anonymous location-based efficient routing protocol in manets," *IEEE Transactions on Mobile Computing*, vol. 12, no. 6, pp. 1079-1093, 2013.

[11] K. Kavitha, K. Selvakumar, T. Nithya, and S. Sathyabama, "Zone based multicast routing protocol for mobile ad hoc network*," in Proceedings of International Conference on Emerging Trends in VLSI, Embedded System, Nano Electronics and Telecommunication System (ICEVENT)*, 2013.

[12] B. A. Mahmood, A. Ibrahim, and D. Manivannan, "Hybrid on-demand greedy routing protocol with backtracking for mobile ad-hoc networks," *in Proceedings of 9th IFIP Wireless and Mobile Networking Conference (WMNC)*, 2016.

[13] H. Yih-Chun and A. Perrig, "A survey of secure wireless ad hoc routing," *IEEE Security Privacy*, vol. 2, no. 3, pp. 28-39, 2004.

[14] J. Luo, M. Fan, and D. Ye, "Black hole attack prevention based on authentication mechanism," *in 2008 11th IEEE Singapore International Conference on Communication Systems. IEEE*, pp. 173-177, 2008.

[15] H. Kalkha, H. Satori, and K. Satori, "Preventing black hole attack in wireless sensor network using hmm," *Procedia Computer Science*, vol. 148, pp. 552-561, 2019.

[16] A. K. Abdelaziz, M. Nafaa, and G. Salim, "Survey of routing attacks and countermeasures in mobile ad hoc networks*," in Proceedings of IEEE International Conference on Computer Modelling and Simulation (UKSim),* pp. 693-698, 2013.

[17] R. Skaggs-Schellenberg, N. Wang, and D. Wright, "Performance evaluation and analysis of proactive and reactive manet protocols at varied speeds," *in 2020 10th Annual Computing and Communication Workshop and Conference (CCWC)*, pp. 0981-0985, 2020.

[18] Vaithiyanathan, G. S. R., E. E. N., and S. Radha, "A novel method for detection and elimination of modification attack and ttl attack in ntp based routing algorithm," *in Proceedings of International Conference on Recent Trends in Information, Telecommunication and Computing (ITC)*, pp. 60-64, 2010.

[19] A. Ibrahim, B. Mahmood, and M. Singhal, "A secure framework for sharing electronic health records over clouds," *in 2016 IEEE International Conference on Serious Games and Applications for Health (SeGAH). IEEE*, pp. 1-8, 2016.

[20] N. W. Lo, M. C. Chiang, and C. Y. Hsu, "Hash-based anonymous secure routing protocol in mobile ad hoc networks," *in Proceedings of Asia Joint Conference on Information Security (AsiaJCIS)*, pp. 55-62, 2015.

[21] A. Ibrahim, B. Mahmood, and M. Singhal, "A secure framework for medical information exchange (mi-x) between healthcare providers," *in 2016 IEEE International Conference on Healthcare Informatics (ICHI)*. IEEE, pp. 234-243, 2016.

[22] I. Woungang, S. K. Dhurandher, M. S. Obaidat, and R. D. Peddi, "A dsr-based routing protocol for mitigating blackhole attacks on mobile ad hoc networks," *Security and Communication Networks*, vol. 9, no. 5, pp. 420-428, 2016.

[23] P. Joshi, "Security issues in routing protocols in manet at network layer*," Procedia Computer Science*, vol. 3, pp. 954-960, 2011.

[24] B. Mahmood, A. Ibrahim, and D. Manivannan, "Sariadne: A secure source routing protocol to prevent hidden-channel attacks," *in Proceedings of 12th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob), IEEE*, pp. 1-7, 2016.

[25] C. E. Perkins and E. M. Royer, "Ad-hoc on-demand distance vector routing," *in Proceedings of Second IEEE Workshop on Mobile Computing Systems and Applications, WMCSA*, pp. 90-100, 1999.
[26] K. Arathy and C. Sminesh, "A novel approach for detection of single and collaborative black hole attacks in manet," *Procedia Technology*, vol. 25, pp. 264-271, 2016.
[27] A. K. Jain, V. Tokekar, and S. Shrivastava, "Security enhancement in manets using fuzzy-based trust computation against black hole attacks," *in Information and Communication Technology. Springer*, pp. 39-47, 2018.
[28] S. R. M. Krishna, P. V. K. Prasad, M. N. S. Ramanath, and B. M. Kumari, "Security in manet routing tables with fmnk cryptography model," *in Proceedings of International Conference on Electrical, Electronics, Signals, Communication and Optimization (EESCO)*, pp. 1-7, 2015.
[29] Proceedings of International Conference on Electrical, Electronics, Signals, Communication and Optimization (EESCO), 2015.
[30] Y.-C. Hu, A. Perrig, and D. B. Johnson, "Ariadne: A secure on-demand routing protocol for ad hoc networks," *Wireless networks*, vol. 11, no. 1-2, pp. 21-38, 2005.

BIOGRAPHIES OF AUTHORS

Dr. Baban A. Mahmood is currently the chairman of Networks Department at University of Kirkuk, Kirkuk, Iraq. He received a B. Sc, degree in Computer and Software engineering from University of Al-Mustansryah, Iraq, in 2003 and a M.Sc., degree in Computer Science from University of Sulaimaniya, Iraq, in 2009. He received a PhD degree in Computer Science from University of Kentucky, Lexington, Kentucky, USA 2016. He worked in the program of some international conferences. He reviewed many papers for several prestigious journals and conferences. He published his research work in the following areas: routing in ad hoc networks, security of source routing protocols in MANET, and security of health records via cloud.

Aso Ahmed Majeed is currently an instructor at University of Kirkuk Kirkuk, Iraq. He received a B.Sc. in software engineering from Technical College, Kirkuk, Iraq in 2004 and M.Sc. in Computer Engineering from Cankaya University, Ankara, Turkey in 2015. He published his research in the following areas: computer networks, security in wireless sensors network, and AI.

Asst. Prof. Dr. Ahmed Chalak Shakir is currently the dean of the College of computer science and information technology, University of Kirkuk, Iraq. He received a B. Sc, degree in Computer and Software Engineering from University of Al-Mustansryah, Iraq, in 2001. In 2002 he got a High Diploma degree in software engineering from Iraqi commission for computers & informatics/ Institute for post graduate studies in informatics, Bagdad, Iraq, and a M.Sc., degree in Computer Science from University of Sulaimaniya, Iraq, in 2007. He also received a PhD degree in Computer Engineering, Harbin institude of technology, china in 2013. He published his research work in the following areas: information and network security.