BLACK HOLE ATTACK SECURITY ISSUES, CHALLENGES & SOLUTION IN MANET

Muneer Bani Yassein, Ismail Hmeidi, Yaser Khamayseh
Mohammad Al-Rousan, Danah Arrabi

Faculty of Computer & Information Technology, Jordan
University of Science and Technology, Irbid, Jordan

ABSTRACT

MANET (Mobile Ad-hoc Network) is simply a set of mobile hosts connected wirelessly without any centralized management, where each node acts as a packet sender, packet receiver, and a router at the same time. According to the nature of this network, the dynamic topology and the absence of a centralized management cause several security issues and attacks, such as the black hole attack, the wormhole attack, and the impersonation and repudiation attack. In this survey, we are going to introduce the Black Hole attack security issues and some of the detection techniques used to detect the black hole attack. In this kind of attack (black hole attack) the intruders manipulate the normal behavior of the network, by introducing themselves as the node with the shortest path to the destination. Intruders can do a malicious behavior over the network.

KEYWORDS

MANET, Routing Protocols, Black Hole Attack, AODV, DSR, RREQ, RREP, RERR.

1. INTRODUCTION

MANET is a group of mobile nodes, where each node has a wireless transmitter and a receiver. the nodes communicate together directly or indirectly [1]. Nodes that are in the same radio range communicate with each other through a direct wireless link; which is known as a single-hop network. In a multi-hop network, if one node wants to communicate with a node that is located out of its range, it relies on the intermediate nodes to transfer the data through it to the required destination [1] [2].

The exposed wireless transmission medium, the changing topology and the lack of main management and controlling unit makes the mobile ad-hoc network vulnerable to different kinds of attacks [1-3]. The changing scalability, the limited power supply and the lack of security boundaries that exist in MANETs make it also a subject of attacks [2]. In MANET, the attacks can be either active or passive.

In passive attacks, the attacker does not affect or modify the data transmitted between communicating nodes. it just listens to the traffic between two nodes looking for valuable data to steal it [4]. Such kind of attacks are hard to discover. As an example: traffic monitoring and releasing of message contents. Active attacks are sensitive and dangerous because it aims to change the normal functionality of the network. changing and altering the transmitted data or even sending false replies [4]. As an example: network Jamming, denial of service,

Dhinaharan Nagamalai et al. (Eds) : CSEIT, NCS, SPM, NeTCoM - 2018
pp. 199–207, 2018. © CS & IT-CSCP 2018 DOI : 10.5121/csit.2018.81815

impersonating, and black hole attack. From Table 1. The attacks in MANET networks occur on different protocol layers [23-27]:

Table 1. The attacks in MANET networks occur on different protocol layers.

Layers	Attacks
Multilayer Attack	DOS, Impersonation, Reply, Man in the middle.
Application Layer	Repudiation, Date corruption.
Transport Layer	Session hijacking, SYN flooding.
Network Layer	Worm whole, Black whole, Flooding, Location disclosure.
Data link Layer	Traffic analysis Monitoring, Disruption MAC, WEP weakness.
Physical Layer	Jamming, Interception, Eavesdropping.

Now, we introduce some of the most important attacks in MANETs. In Black Hole Attack, the attacking node abuses the routing protocol used in the network to introduce itself as the node that has the shortest path to the destination node. attacking node attracts all packets towards it. This malicious node discards packets without forwarding it to any other nodes[2][3]. In Worm Hole Attack, the malicious node records packets at one point inside the network and then delivers them to another location [2][3]. In Byzantine Attack, the attacking node inserts wrong routing information into the network to create routing loops. forwarding packets through wrong and non-optimal paths or dropping packets cause problems in the routing functions [3]. in this survey, we focus on the Black Hole Attack.

This paper is organized as following: section 2 discusses the MANETs' routing protocols, Section 3 discusses the concept of black hole attack, Section 4 discusses some recent detection schemes, and section 5 is the conclusion.

2. ROUTING PROTOCOLS IN MANETS

A The routing protocol is a set of rules and conventions that govern the movement of data within the network and choose the path that the data packets should travel through to reach the desired destination. A routing protocol also determines the way the router interacts with other routers. First, the routing protocol podcasts the routing information to the direct neighbors and then this information propagated through the network. Setting up the optimal route (minimum hops) between the source node and the destination node, so that the data packets reach the destination in a well-timed manner with no waste in the network bandwidth and with the least overhead is the main goal of routing protocols in ad-hoc networks [5]. When a node needs to communicate with other nodes to send data over the network, the current status of this node must be podcasted to the neighbors, where the routing information preserved by each node must be updated due to the nature of MANET [6]. Based on the way this information is collected [5][6], and the measures when the sending node seize a path to the destination (routing strategies) [7], the MANET routing protocols can be classified into three main categories:

2.1. TABLE-DRIVEN (PROACTIVE) ROUTING PROTOCOLS

Proactive protocols preserve up-to-date and consistent routing information related to every node that exists inside the network topology even before it is needed [5] [8]. Each node constructs its own routing table and deploys this table to find the optimal route to a specific destination [7]. This node needs to preserve an up-to-date and trustworthy information in its routing table [5] [7], not only routing information related to the adjacent nodes, but also about all the nodes that can be reached, in addition, the number of hops that need to reach another node on the network [6].

Whenever there is a change in the network topology, the entire network must be notified about this change. In this case, each node updates its routing table as much as needed so that the routing table remains reliable and consistent. This is done by each node periodically by podcasting its routing table to the neighbors. So whenever something changes the whole network must be notified [5-7] [9] [21] [22].

The disadvantages of this type of protocols are the expanding of the network size and the growing of the communication overhead.as an advantage, this protocol allows the network state to change immediately whenever a malicious node joins the network topology, so an action can be taken [5] [6] [18] [19] [20]. Some of the existing proactive routing protocols are Destination Sequenced Distance Vector routing (DSDV), Wireless Routing Protocol (WRP), Cluster Gateway Switch Routing protocol (CGSR), Fisheye State Routing (FSR), and Optimized Link State Routing (OLSR).

2.2. ON-DEMAND (REACTIVE) ROUTING PROTOCOLS

On-Demand (Reactive) Routing Protocols also known as source-initiated routing protocols, it starts when a node wants to send a message to another node in the network [5] [6], which means that a route to a destination node will be established just when it is required [5] [6] to scale down the overhead in the network [10]. When a specific node wants to send data to a new destination, the Route Discovery Process starts. this process tries to find a route to the destination [7]; the source node broadcast a route request message (RREQ) to the direct nodes connected to it. After the neighbors receive the message they again broadcast the message to their neighbors, and so on until the message delivered to the destination. The destination, in The node preserves information about the active routes to the other nodes in the network. But the discovery process is done for each new destination. the nodes that are inactive do not participate in such a process. The newly discovered route is presented in the node's routing table until the route is no longer required [5] [7]. The strength in the reactive routing protocols is reduced of bandwidth that was wasted due to the continued broadcasting of routing tables in other MANET proactive routing protocols. the communication overhead is also reduced, on the other hand. delays may occur due to the route discovery operation. where a new discovery process starts for each new destination. This process considers the main reason for attacks done by malicious nodes. some packets may be lost because of the routing techniques used [6]. Examples of existing reactive routing protocols are: Ad-hoc On-demand Distance Vector routing (AODV), Dynamic Source Routing (DSR), and Temporally ordered routing algorithm (TORA). We discuss AODV and DSR in more details.

In AODV, each node preserves information for the next hop in its routing table. The routing path from source to destination node also saved on routing table [5][6]. There are two main phases in AODV routing protocol: the route discovery and the route maintenance phase [7]. The discovery phase begins when a source node wants to send data to a specific destination node that not exist in routing table [7]. which means that the route to that destination is not known [5] [6].

In this operation, the source node broadcasts an RREQ to all of its neighbors. the neighbor nodes do the same when they receive a new RREQ message. Each node keeps a sequence number and a broadcast ID which is incremented each time the node sends an RREQ message. this process repeats until the message reaches the destination. in this case, an RREP unicasts from that destination back to the source node. once the RREP message is received by the source node, a route from the source node to the destination is built. The RREP message could also be unicasted to the source node if an intermediate node has a fresh-enough route to the destination [5-7], Figure 1 shows the propagation of RREQ and RREP message inside the network.

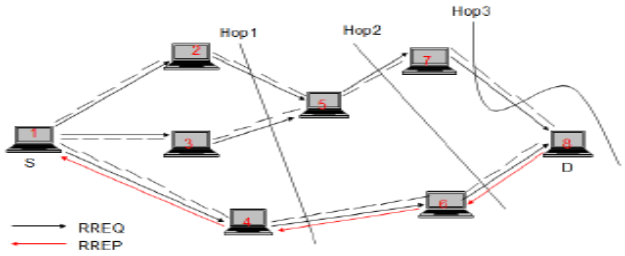

Figure 1 Propagation of Route Request packet & Route Reply packet

The route maintenance phase starts when there is a change in the distribution of the network nodes (topology) or when there is a link broken for a specific routing path between two nodes which means a connection failure[5-7].In this case a route error message (RERR) is propagated inside the network in a reverse direction to reach the source node that is related to that broken route, the intermediate nodes use this message in order to update their routing information, the source node delete the invalid routing information that is related to the broken links from their routing tables[5][11]. Once the RERR message reaches the source node, it starts looking for an alternative route, and if there were no alternative route was found, a new route discovery process starts again [6][7].

Scientists categories this protocol as a pure reactive routing protocol, because the nodes that are not located on a specific path do not preserve routing information related to that path, and do not participate in the swapping of routing tables. the performance of the network decrease as the network grows, with potential overhead caused by RREQ, RREP and RERR messages traveling inside the network during the route discovery process [7].

DSR is a source of routing protocol, which means that the source node decides the full routing path to send the data through it to destination, this is because each node here has a route cache or what it is called known routes, and this the place where each node preserves a routing information about all of the known paths from a source to different destinations [5][6][12], this route cache is altered each time a new route to a destination is known in the network [12]. Unlike AODV where each node preserves information about only the next hop node in their routing tables. Each data packet holds the full path from source to destination in its header [5][6].

the main phases: route discovery and route maintenance. When one node wants to send data packets to a specific destination, it first checks the route cache to see if it knows the destination and to see if there is a route to it. if there is a route information source node sends the data through it. otherwise, it broadcasts a route request packet to the neighbors, and they, in turn, check their route cache to see if there is a route to that destination. if not had the route information the packet is forwarded until the destination is reached. In this case, a route reply message is created. Also, the route reply message is generated if an intermediate node knows a route to a destination [12]. The disadvantage in DSR is that when the mobility of the network nodes increases, the delivery rate and the performance of the network probably decreased [6].

2.3. HYBRID ROUTING PROTOCOLS:

Hybrid Routing Protocols is a kind of routing protocols that combines the features of both proactive and reactive routing protocols in order to defeat the cons of them [6][7]. these routing protocols are designed using a layered framework [5][6]. The nodes of the network are divided into groups, based on the geographical area, and the distance between those nodes [5][7]. The proactive routing technique is used in order to collect the routing information [6] and to establish

communication between the nodes that belong to the same zone [5][7]. while the reactive routing technique is used to keep the routing information when the topology of the network is altered [6] and to establish a connection between the nodes that belong to different zones [5][7]. Some of the existing hybrid routing protocols are: Temporally-Ordered Routing Algorithm (TORA), Zone Routing Protocol (ZRP), Zone-based Hierarchical Link State (ZHLS), and Distributed dynamic routing (DDR).

3. BLACK HOLE ATTACK

Black hole refers to an area in the network that drops the traffic headed to a specific destination through it, without informing the source node that the data packets was not delivered to the destination [5]. In the black hole attack, a node exploits the routing protocol to exhibit itself as the node that has the shortest path to reach a specific destination [5][14][15], after that this node receives the data packets, that supposed to be forwarded to the right destination through this node, now the node drops those packets as type of denial of service (DoS) threat [5], consumes the packets [13][14], or exploits its location in the network to advertise itself as the destination node (man-in-the-middle threat) and starts to redirect different packets inside the network [5].

In such a case, the source and the destination cannot communicate with each other. The black hole nodes here are unseen, and the network traffic must be observed to detect such nodes. In Figure 2, node A wants to send data to node F, it broadcasts an RREQ to the nodes B, M, and D, M is a malicious node, replies with an RREP message implying that it has fresh-enough route to the destination [5][13], this RREP arrives at node A before nodes' B and D RREP, node A assumes that the route discovery process has ended, ignoring all the other RREP messages, and starts to send data packets to node M, which in turn drops those packets [5][13][14][22].

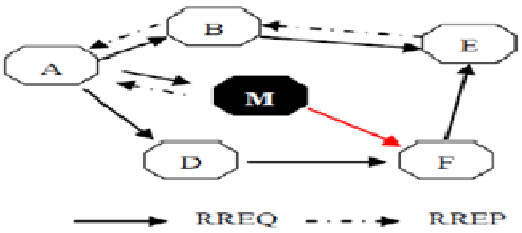

Fig 2: Black hole Attack

The black hole attack can be classified based on the strategy used by the malicious node to perform the attack. the node either drops all the packets that arrive to it which is supposed to be forwarded to the intended destination, or the node chooses some of those packets to drop, which it does not like [5].

The node that plans to attack, must find a way to put itself on the path that control packets or data packets will be delivered through it. relying on some vulnerabilities already exist in the used routing protocol, which was designed on the basis of trustworthiness between the network nodes, every node can do a wrong behavior and sabotage the network operations by destroying the data packets or misuse the control packets [5]. The dropping of packets terminates the communication and transmission between two nodes, what is worse than that is the malicious node preventing the establishing of a route between those nodes [5].

In the AODV routing protocol, the sequence number is used to indicate the freshness of the different network routes. it exists in the message that is received from the source. The more the

larger this sequence number is, the fresher the route related to this number is [5] [14]. When the destination replies with a REPP message, it compares the sequence number inside the (RREQ+1) message delivered to it and the destination's current sequence number, picks the larger one and puts it in an RREP message, and then unicasts it back to the source through the shortest path. When the source receives more than one RREP message it chooses the one with the highest sequence number and sends the data through that path [5] [13] [14].

What happens exactly in AODV routing protocol, is that, when one node has no fresh-enough route to a specific destination and wants to send data to it, it broadcasts an RREQ message to all of the neighbors, if these nodes has a fresh-enough route to the destination they reply with an RREP message to the source. In turn, the source uses the RREP message that holds the highest sequence number and drops the rest of them. After that, it starts to send the data. In the case of a multiple RREP messages holding the same sequence number, the source uses the one that holds the smallest hop count and starts to send the data through that shortest path [14]. When a node intends to perform a black hole attack, when a source node broadcasts an RREQ message to nodes, the black hole node replies with an RREP message that holds the highest sequence number, this message is delivered to the source node as if it was from the destination, or from a node that has a fresh-enough route to the intended destination, as a result, the source drops all the other RREP messages, and starts sending the data packets to the black hole node. Trusting that the data will be delivered to the correct destination. So, the black hole node attracts all the data towards it and then discards or consumes them, and they will be never delivered to the destination [13-15].

In order to succeed in the attack, the node must create a route reply message with a sequence number larger than the current sequence number to absorb all the packets and then discards them [5]. Black hole attacks can be classified based on the way of the attack perform [15] into two main types: Simple or Single Black Hole Attack (ordinary)[14][15], and Collaborative Black Hole Attack, in which, two or more nodes collaborate, to manipulate the routing information to hide from the detection mechanisms [14] or to form a team that prevents the data from reaching a specific node, and its much more dangerous than the first type because it is hard to detect and easy to be performed. where one malicious node sends the data to another malicious node that, in turn, swallows the data packets without forwarding those [15].

Black hole attack degrades the network performance, causing a low packet delivery ratio, less throughput, and disturbing the route discovery process [5] [13] [14].

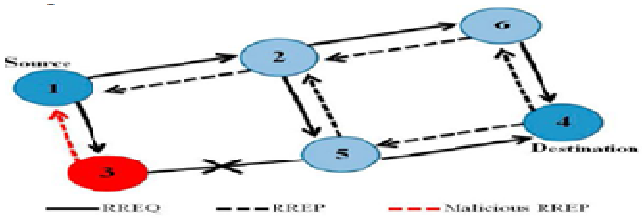

Figure 3 The single black hole problem

4. PROPOSED DETECTION SCHEMES

In this section, we will discuss some of the black hole detection schemes that were proposed in the last few years

.

4.1. ENHANCED AODV ROUTING PROTOCOL

In 2014, Bani-Yassin et al. [16] proposed an improved AODV routing protocol to detect and avoid the black hole attack in MANETS. They suggested that the RREP message should be monitored along with its history, through the addition of a new field to its structure that contains the address of the last node that has a route to a specific destination. In addition monitoring of the node's behavior in the network by adding two tables inside each node one is called the suspect table and the other is called the blacklist table. The suspect table contains a list of nodes addresses from which they received an RREP messages, and the number of failed RREP messages arrived from each node in the list. The RREP message is considered to be failed when a specific source fails to send data through the path related to this message. Which means that the source did not receive any acknowledgment. While the Blacklist table contains the addresses of nodes that exceeds a certain number of failed RREP messages. Each node that has been moved from suspect list to this list, all the RREP messages arriving from it will be ignored by other nodes in the network. And the last modification is the creation of a 1-bit sized ACK message that is set to 1 if the data arrived at the destination otherwise they are set to 0, and they will be propagated back to the source.

They did a simulation of a MANET network to evaluate the performance of the standard AODV, MI-AODV, and evaluate the proposed AODV with the presence of 1,2 and 6 black hole nodes in the network. The evaluation metrics used are the packet delivery ratio, dropped packets ratio, delay, and network overhead. The packet delivery ratio increased by 50.9% with the presence of 1 black hole node and by 57.8% with the presence of two black hole nodes when using the proposed AODV routing protocol compared to the standard AODV, with many nodes scaling from 15 to 35 nodes. The dropped packets ratio decreased by 61.5% with the presence of 1 black hole node and by 57.8% with the presence of two black hole nodes when using the proposed AODV routing protocol compared to the standard AODV, with a number of nodes scaling from 15 to 35 nodes. But when it comes to the delay times, the proposed AODV achieves the highest delay compared to the standard AODV and MI-AODV and this because of the time is taken to process and deliver the packets through an alternative route after the first route fails to do that, because of the presence of a black hole node. Also, the proposed AODV achieved the lowest overhead compared to the other two protocols.

4.2. TIMER BASED DETECTION MECHANISM

Choudhary and Tharani [17] suggested that each node in the network set a new value to all the neighbor nodes. This value is called the maximum trust value. As we all know, the source node starts sending the data to the first neighbor node that is send the RREP message, according to the proposed method, when the source node (N) sends the data to the neighbor (N+1) that is one hop away, it sets a timer (T) in seconds, and when this timer expires the node (N) starts listening to the medium to see if it has been received the same data it has sent to node (N+1), if node (N) did not hear anything it decreases the trust value related to node (N+1) by 1, and this information is propagated inside the whole network so that the other nodes update the trust information entries related to that node in their tables, and when the trust value of a node becomes less than a predefined min trust value, it will be blacklisted and all the messages and actions coming from this node will be ignored. We should point out that the time (T) is the total packet processing in time.

They used the packet delivery ratio as a measure to evaluate their mechanism, and they have approved that their proposed solution increasing the packet delivery ratio compared to the packet delivery ratio in a black hole infected AODV. Table (2) shows a comparison between the two detection schemes.

Table 2. Comparison between the two detection schemes.

Schemes	Enhances AODV	Time-Based Mechanism
Routing Protocol	AODV	AODV
Simulator	GloMoSim	EXata-cyber
Year	2014	2015
Evaluation metrics	PDR, DPR, Delay, Overhead	PDR
Strengths	Higher PDR, lower DPR, and overhead	Higher PDR
Weaknesses	Higher delay	More evaluation metrics should have been used

3. CONCLUSION

MANET networks are networks with a dynamic topology that comes with a lot of security and attacks issues. One of the major attacks is the Black Hole Attack that exploits the used routing protocol to harm the normal operations of the network. Every day a new detection and prevention schemes are being proposed by researchers over the world to overcome this problem. By detecting this attack or at least mitigate the negative effect of it, we will help in preserving good and secure networks for exchanging knowledge and experiences around the world.

REFERENCES

[1] Suresh, M., & Shaik, S. (2016). Security Issues in MANETS. International Journal, 4(2).

[2] Ishrat, Z. (2011). Security issues, challenges & solution in MANET. IJCST, 2(4), 108-112.

[3] Priya, S. B., & Theebendra, C. (2016). A STUDY ON SECURITY CHALLENGES IN MOBILE ADHOC NETWORKS.

[4] Garg, A., & Beniwal, V. (2012). A review on security issues of routing protocols in mobile ad-hoc networks. International Journal of Advanced Research in Computer Science and Software Engineering, 2(9).

[5] Ahmed, A., Hanan, A., & Osman, I. (2016). Description of Black Hole Attack Behaviour in MANET. International Journal of Computer Networks and Communications Security, 4(12), 322.

[6] Tseng, F. H., Chou, L. D., & Chao, H. C. (2011). A survey of black hole attacks in wireless mobile ad hoc networks. Human-centric Computing and Information Sciences, 1(1), 4.

[7] Kumar, J., Kulkarni, M., & Gupta, D. (2013). Effect of Black hole Attack on MANET routing protocols. International Journal of Computer Network and Information Security, 5(5), 64.

[8] Jayakumar, G., & Ganapathy, G. (2007). Performance comparison of mobile ad-hoc network routing protocol. International Journal of Computer Science and Network Security (IJCSNS), 7(11), 77-84.

[9] Shrivastava, P., Kumar, S., & Kumar, M. (2014). Study of Mobile Ad hoc Networks. International Journal of Computer Applications, 86(3).

[10] Bai, F., Sadagopan, N., Krishnamachari, B., & Helmy, A. (2004). Modeling path duration distributions in MANETs and their impact on reactive routing protocols. IEEE Journal on Selected Areas in Communications, 22(7), 1357-1373.

[11] Hinds, A., Ngulube, M., Zhu, S., & Al-Aqrabi, H. (2013). A review of routing protocols for mobile ad-hoc networks (manet). International journal of information and education technology, 3(1), 1.

[12] Prakash, S., Kumar, R., Nayak, B., & Yadav, M. K. (2011). A Survey on Reactive Protocols for Mobile Ad Hoc Networks (MANET). In Proceedings of the 5th National Conference (pp. 10-11).

[13] Kakoty, B. S. (2013). Simulation and Analysis of Blackhole Attack in MANETs for Performance Evaluation. International Journal of Latest Trends in Engineering and Technology (IJLTET) Vol, 2.

[14] Bhattercharjee, A., & Paul, S. A Review on some aspects of Black Hole Attack in MANET. network, 1, 2.

[15] Al Dulaimi, L., Ahmad, R. B., Hassnawi, L. A., & Ahmed, I. (2016). Black Hole Malicious Behaviour via Different Detection Methods

[16] BaniYassein, M., Khamayseh, Y., & Nawafleh, B. (2014). Improved AODV Protocol to Detect and Avoid Black Hole Nodes in MANETs. FUTURE COMPUTING, 7-12.

[17] Choudhary, N., & Tharani, L. (2015, January). Preventing black hole attack in AODV using timer-based detection mechanism. In Signal processing and communication engineering systems (SPACES), 2015 international conference on (pp. 1-4). IEEE.

[18] Bader, A., Mardini, W., & Yasein, M. B. (2011). A new protocol for detecting black hole nodes in ad hoc networks. International Journal of Communication Networks and Information Security (IJCNIS), 3(1).

[19] Qasem, M., Altawssi, H., Yassien, M. B., & Al-Dubai, A. (2015, October). Performance evaluation of RPL objective functions. In Computer and Information Technology; Ubiquitous Computing and Communications; Dependable, Autonomic and Secure Computing; Pervasive Intelligence and Computing (CIT/IUCC/DASC/PICOM), 2015 IEEE International Conference on (pp. 1606-1613). IEEE.

[20] Yassein, M. M. B., Khaoua, M. O., Mackenzie, L. M., & Papanastasiou, S. (2006, September). Performance evaluation of adjusted probabilistic broadcasting in MANETs. In Dependable, Autonomic and Secure Computing, 2nd IEEE International Symposium on (pp. 245-249). IEEE.

[21] Khamayseh, Y., Al-Salah, R., & Yassein, M. B. (2012). Malicious nodes detection in MANETs: behavioral analysis approach. Journal of networks, 7(1), 116.

[22] Yassein, M. B., Al-Dubai, A., Khaoua, M. O., & Al-Jarrah, O. M. (2009, May). New adaptive counter based broadcast using neighborhood information in manets. In Parallel & Distributed Processing, 2009. IPDPS 2009. IEEE International Symposium on (pp. 1-7). IEEE.

[23] Yassein, M. B., & Aljawarneh, S. (2017). A new elastic trickle timer algorithm for Internet of Things. Journal of Network and Computer Applications, 89, 38-47.

[24] Yassein, M. B., Mardini, W., & Khalil, A. (2016, September). Smart homes automation using Z-wave protocol. In Engineering & MIS (ICEMIS), International Conference on (pp. 1-6). IEEE.

[25] Charalambous, M. C., Mavromoustakis, C. X., & Yassein, M. B. (2012, June). A resource intensive traffic-aware scheme for cluster-based energy conservation in wireless devices. In High Performance Computing and Communication & 2012 IEEE 9th International Conference on Embedded Software and Systems (HPCC-ICESS), 2012 IEEE 14th International Conference on (pp. 879-884). IEEE.

[26] Yassein, M. B., & Hijazi, N. (2010, July). Improvement on cluster based routing protocol by using vice cluster head. In Next Generation Mobile Applications, Services and Technologies (NGMAST), 2010 Fourth International Conference on (pp. 137-141). IEEE.

[27] Yassein, M. M. B., Khaoua, M. O., Mackenzie, L. M., & Papanastasiou, S. (2006, September). Performance evaluation of adjusted probabilistic broadcasting in MANETs. In Dependable, Autonomic and Secure Computing, 2nd IEEE International Symposium on (pp. 245-249). IEEE.