Bait Request Algorithm to Mitigate Black Hole Attacks in Mobile Ad Hoc Networks

Ayanwuyi T. Kolade, Megat F. Zuhairi, Hassan Dao, Sohail Khan

Universiti Kuala Lumpur, Malaysian Institute of Information Technology, Jalan Sultan Ismail, 50250 Kuala Lumpur, Malaysia

Summary

In the recent years the number of mobile device have significantly increase and the high bandwidth have led to the demand for Mobile Ad hoc Network (MANET). The network offers mobile access to users with minimal configuration to operate. Nonetheless, such salient feature requires flexibility and cooperation between users, which increases the network's vulnerability to the Black hole attack. Therefore, an improved security approach is needed to maintain optimal network performance. The Black hole attack can severely threaten the network by exploiting the vulnerability of Route Request (RREQ) discovery process in the routing protocols such as Ad hoc On Demand Distance Vector (AODV). The intruders are able to utilise the loophole and carry out the malicious behaviours because the RREQ process is an essential mechanism within AODV. As a result, genuine RREQ packets are exploited and erroneously relayed to a false node(s). The on demand routing protocols, which act as the binding element in the networks, are a common target to such security attack. This paper presents a review of the Black hole attack on mobile nodes and subsequently proposes a new mechanism to alleviate the issue. The AODV routing protocol is chosen as the base protocol because it is inherently similar to other types of on demand routing protocol e.g. DSDV, DSR. In fact, any routing protocol which follows the request-reply method may utilise the scheme to mitigate the issue. It includes the proactive routing protocol such as OLSR. In the proposed scheme, each node is capable to detect and isolate the malicious node in their local region with appropriate implementation.

Key words:

MANET, AODV, Black Hole, Malicious node, Network Security, Wireless network

1. Introduction

To date, wireless module is an essential element, which is seamlessly embedded within any mobile devices. Each mobile device typically communicates with using wireless network i.e. Wi-Fi, cellular network. The coding scheme and modulation technique of such technologies have been significantly improved to the extent that the access speed can support real time application. Additionally, the technology allows for instant Internet connectivity for mobile users anywhere and anytime. The wireless connectivity is also convenience for mobile users to be connected instantly to the network with acceptable network performance.

Generally, a MANET consists of mobile nodes that use wireless transmission for communication. In MANET the nodes are able to move from one location to the other. The motion of the mobile nodes may be random or follows a specific periodical pattern [1]. Despite mobile, nodes in MANET can spontaneously establish routes and relay packets. Receiver nodes that are outside the radio range of the source nodes receive packets by means of relay. Therefore, nodes in MANET not only act as ordinary network nodes but also as the routers for other peer devices.

Due to the unique characteristics of MANET and the low demand for fixed infrastructure, the development of a permanent intrusion detection system is quite challenging. The absence of a centralised gateway device to monitor the network traffic exposes the network to potential security attack. The inherent nature of broadcast traffic in wireless communication has led to both legitimate and malicious nodes to access the network. To that end, the fundamental issue of MANET is to ensure data can be securely delivered and efficiently among the mobile nodes. Additionally, the network's topology frequently changes. Consequently, a secure routing is difficult to achieve in a MANET due to the additional packet overhead concern. Although many high performances routing protocol offers optimal performance, the security aspect is often neglected. Therefore, to improve the success of packet delivery it is essential that a mobile routing protocol have the ability to secure its route connection.

Numerous studies have attempted to improve security methods for on demand routing protocol. Nevertheless, many has failed because of the failure to accommodate the dynamic attributes of MANETs i.e., topology, different network sizes, varying battery capacity, error prone medium, power, storage and computational resources. Such challenges have made it difficult for previous researchers to design a fixed and efficient routing protocol.

Manuscript received May 5, 2016
Manuscript revised May 20, 2016

In this paper, five different types of attack typically found in MANET are discussed.

1.1 Wormhole attack

In a wormhole attack, a potential attacker receives packets at one point in the network and tunnels them to another point in the network. Later the packets are replayed into the network from the last point received. The tunnel between two colluding attacks is known as a wormhole. The tunnel i.e. wormhole creates a private path which effectively propagates packets concealing the malicious activity. At the other end of the network the packet is then replayed. The network can be severely affected causing suboptimal routing performance.

1.2 Sinkhole attack

In a sinkhole attack, a compromised node attempts to attract data from the neighbouring nodes. It is done by promiscuously eavesdrops each data that is being communicated between its neighbouring nodes. Upon receiving the data, the packets are dropped causing high network loss and packet retransmission by the source node.

1.3 Gray-hole attack

This attack is also known as routing misbehaviour attack which leads to dropping of messages. The gray-hole attack has two phases. In the first phase, the node advertises as having a valid route to destination while in the second phase, the node drops intercepted packets with a certain probability.

1.4 Replay attack

It is a malicious attempt by the attacker, which collects data and routing packets. Later the collected packets are replayed. Such attack may cause a network to be falsely detected and it allows unauthorised users to impersonate a different node identity. Typically such method is used to gain access to data which was demanded by replayed packet.

1.5 Black hole attack

The attacker advertises a zero metric for all destinations, leading to all nodes in the proximity to route packets towards it. A malicious node sends fake routing information, claiming it has an optimum route and causes other nodes to route data packets through the malicious one. Subsequently, each packet routed through the malicious node is dropped.

The aim of this paper is twofold. First is to present several types of security flaws which are comparable to Black hole. Secondly is to present and improved algorithm to on demand routing protocol against the Black hole attack. The AODV routing protocol is chosen due to the fact it fulfil the on demand routing behaviour. It is also equipped with both unicast and multicast routing capabilities. The paper is organised as follows. Section 2 provides an overview of AODV routing protocol and discusses the Black Hole nodes. Section 3 presents previous research work. Section 4 presents the proposed method. Section 5 discusses the security analysis and finally, Section 6 concludes the paper.

2. AODV and Black hole Nodes

2.1 AODV Routing Protocol

AODV is classified as a reactive routing protocol. It is one of the most well-known protocols in MANET, which inherits some of the features of Destination Sequenced Distance Vector (DSDV) routing protocol. In contrary to DSDV, the AODV route request procedure is modified to minimise the number of broadcasts. The routes are established on-demand compared to DSDV, where complete lists of routes are maintained upon the first route request [2]. The AODV routing protocol is proposed by Perkin et al. and the algorithm is standardised in document IETF RFC 3561 in 2003. Similar to DSDV, the AODV routing protocol employs the destination sequence number to maintain each route entry. Prior to broadcast, the destination sequence number is generated by the destination node. To maintain fresh path, the requesting node selects the route based on packet that carries the greatest sequence number. Basically, the AODV has three message types, which are RREQs, Route Replies (RREPs), and Route Errors (RERRs). Upon receiving the RREQ, a node first checks in its routing table for existing path back to the sender. If such path does not exist, the node then generates an entry for a reverse route. On the other hand, if the node’s table shows a valid reverse route entry but the sequence number is less than the source sequence number in the RREQ (a larger number means fresher information), the current reverse route entry is changed with the information in the RREQ. If a node has a path to the destination, and the route is not expired, the node will instantly reply with unicast RREP packet back to the source by using the reverse path. Nevertheless, the RREQ will continue to be propagated until it reaches the destination. Note that the destination node will follow the same mechanism as previously stated when it receives the RREQ packet [1][3][4].

2.2 Black Hole Nodes

Black hole attack can severely deteriorate the MANET and it is performed by a single node or a combination of nodes [5]. In an ad-hoc network that uses the AODV protocol, a black hole node pretends to have fresh routes i.e., greatest sequence number to all destinations requested by the sender eventually absorbs the network traffic. When a source node broadcasts the RREQ packet, the black hole node immediately responds with an RREP message that includes the highest sequence number, which is perceived originates from a genuine destination or from a node which has a fresh enough route to the destination. The source assumes that the destination is behind the black hole node and discards other incoming RREP packets. When the source node receives the RREP packet, it then starts to send out the data packets to the black hole node trusting that these packets will reach the destination. Eventually, the data packet is dropped and not propagated further to the genuine destination.

As shown in Figure 1, the source node 0 broadcasts an RREQ message to discover a route to the destination node 2. An RREQ broadcast from node 0 is received by neighbouring nodes 1, 3 and 4. However, as soon as the request packet is received by the malicious node 4, it sends an RREP packet despite the absence of valid path to the destination node 2. Assuming the RREP message from the malicious node 4 is the first to arrive; the source node updates its routing table for the new route to the particular destination node and discards any RREP message from other neighbouring nodes including the one from the actual destination node. Once the source node stores a route, it starts sending data packets to a malicious node expecting that the data will reach the intended destination node. Nevertheless, the malicious node (performing a black hole attack) drops all data packets rather than relay to the next hop node [2].

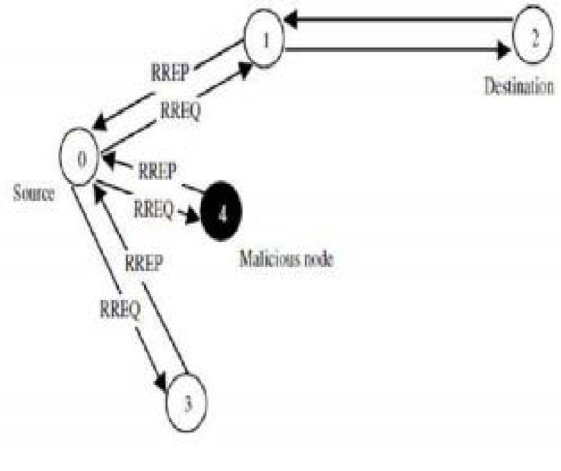


Fig 1: Broadcasting RREQ

3. Related Works

This section discusses various methods other researches have proposed to prevent the black hole attack in MANET. Mehdi Medadian et al [6] employed an approach where the node uses number rules to infer about the trustworthiness of sender's reply packet. The activities of a node are logged by its neighbours. The neighbours are periodically requested to send update their opinion about the neighbour node. When a node collects all opinions from its neighbours, it may be able to decide if the replier is a malicious node. Generally, the decision is made based on a number of rules. A malicious node can be judged based on the node's activity in a network. The first rule implies that if a node delivers many data packets to destinations, it is assumed as an honest node. According to second rule, if a node receives many packets but does not send the same data packets, it may be possible that the node is misbehaving. Additionally, the second rule is insufficient to justify a node is being malicious. To verify that the node is indeed misbehaving, the node has to send a number of RREP packets. When such criterion is fulfilled, the current node is considered a failed node.

S. Tamilarasan [7] proposed a method where the algorithm checks the discrepancy between the sequence number of the source nodes and the intermediate node that has returned the RREP. Typically, the first request reply packet table is from the malicious node with high destination sequence number. In other words, the method compares the first destination sequence number with the source sequence number. If the difference is high, then the destination node may be potentially a malicious node. Later the entry can be directly eliminated from the RR-Table. The main benefits of the proposed solution are that the malicious node is identified at the initial stage itself and immediately removed to prevent further participation in routing process. The method is also able to proactively identify malicious node with minimum delay and disruption to the network.

M Zaveri et al [8] proposed additional overhead to the existing AODV algorithm. The method introduces additional data structures to the existing AODV scheme which includes Cmg_RREP_Tab, a timer MOS_WAIT_TIME and a variable Mali_node. In this scheme, the source node waits for MOS_WAIT_TIME after receiving the first RREP message. Within this time, the source node records each RREP control messages in the Cmg_RREP_Tab table. The MOS_WAIT_TIME is defined to be the half the value of RREP_WAIT_TIME, which is the time the source node waits for RREP control messages before regenerating the RREQ packet. Subsequently, the source node analyses the stored RREPs from Cmg_RREP_Tab table, and discards every RREP with presumably high destination sequence number. The proposed scheme marked the node that sent such RREP as a suspect for being a malicious node. When such node is identified, the reply record with the highest destination sequence number is selected from Cmg_RREP_Tab table. The identity of the malicious node is maintained as Mali_node. As a result, any future communication with the Mali_node can be immediately recognized and discarded.

Govind Sharma et al [9] proposed an approach, where initially the source node broadcasts the route request packet to search the route to the destination node. The source node then initialises the timer in the route request packet to check the route reply time out. In AODV packet routing, every intermediate nodes with a valid route to the destination, or destination node itself, are allowed to send the route reply to the source node. In this algorithm, when the route reply is sent from the final destination, then the route is assumed to be safe and the data can be routed through the path. A route reply packet from intermediate node (named as nth node), in this case by analysing accumulated path nodes (APN) count field i.e. the number of accumulated path nodes appended to the RREP, nodes that are one hop (named as x) before of this nth node will be on its promiscuous mode packet so that they can overhear the route of nth node. After that x will send the plane packet to destination node through node n to check either nth node forwarding the data or not. If the nth node drops the plane packets then x will broadcasts the alarm to all other nodes to inform that there is a malicious node in the network otherwise the nth node is a trusty node.

4. Methodology

Figure 2 shows when a source has data to transmit to an unknown destination; it broadcasts a RREQ packet for that destination. At each intermediate node, when a RREQ is received, a reverse route to the source is created. If the receiving node has not previously received the RREQ, not the intended destination and does not have a current route to the destination, it rebroadcasts the RREQ. In contrast, when the receiving node is the destination or has a current route to the destination, it generates a RREP packet. The RREP is unicast in a hop-by-hop fashion to the source. As the RREP packet propagates, each intermediate node creates a route pointing to the destination. When the source receives the RREP packet, it records the route to the destination and can begin sending data. If multiple RREPs are received by the source, the route with the shortest hop count is chosen [10].

5. Bait Request Method

The proposed method requires each node to detect and isolate the attackers in its local neighbourhood. The proposed solution improves the AODV scheme twofold. In the first mechanism, the security of the route discovery phase of the AODV routing protocol is improved by detecting the black hole nodes. A black hole node will always respond to any route request that reaches it by sending a fake reply. A fake reply is when the malicious node send instantly return a RREP packet despite its routing table is void. The node will also set the destination sequence number of the RREP packet to a maximum possible value and the hop count field to unity. However, the sequence numbers are typically incremented by a node each time a packet is received and processed. As a result, in many ad hoc networks, the sequence numbers may easily build up due to large number of nodes with numerous amounts of control and data exchanges. In such cases, it is possible for a genuine node to generate a RREP packet with high sequence number. Therefore, when a suspicious reply is received, additional checks must be performed to determine the possibility the RREP is sent by a malicious node.

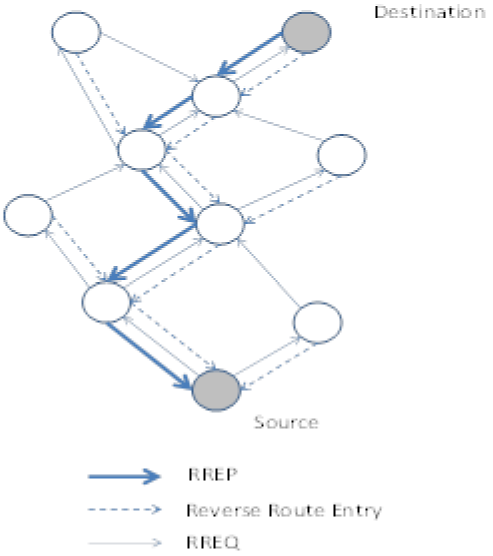


Fig 2: AODV packet transmission process

In the first Bait Request algorithm, when an intermediate node receives a RREP packet, it parses the value and checks whether the destination sequence number of the RREP is maximum and hop count is minimum. If the value matches, the received RREP packet is buffered and a local detection scheme is initiated. The intermediate node creates a bait request packet (BRQ). The destination address of the bait RREQ is set to one of the known neighbour address of the intermediate node. The TTL of the packet is set to 1 to limit the propagation in the local neighbourhood. The packet is then broadcast to the all downstream neighbours. The intermediate node will collect the RREP received for the bait packet. The node then compares the sequence number in the bait reply (BRP) received from the suspected node and that from the known neighbour (original destination node of the bait RREQ). If the destination-sequence-number of the RREP from the suspected node is larger than original destination-sequence-number, the suspected node is malicious. The previously buffered RREP is then discarded. The suspected node is then added to the malicious list and alert packet is propagated across the network.

As illustrated by Figure 3 and the pseudocode in Figure 4, when IN receives a suspicious reply, it sends BBREQ to all neighbours except the one from which it received the original RREQ. A, B, E, F and C are the one-hop neighbours of the current intermediate node IN. The destination address of BRQ can be randomly set to any of the A, B, C, E, and F. In this stage, each BRP received for the BRQ can be checked in the similar way to detect other misbehaving nodes the neighbourhood of the intermediate node.

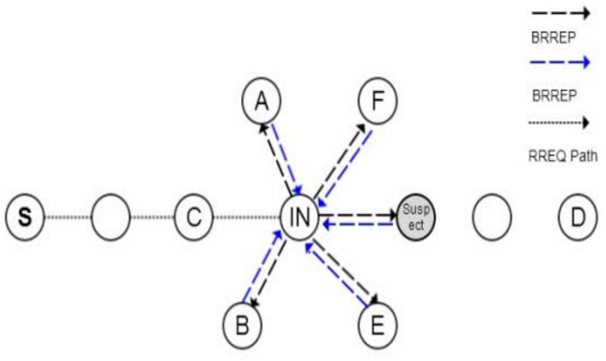
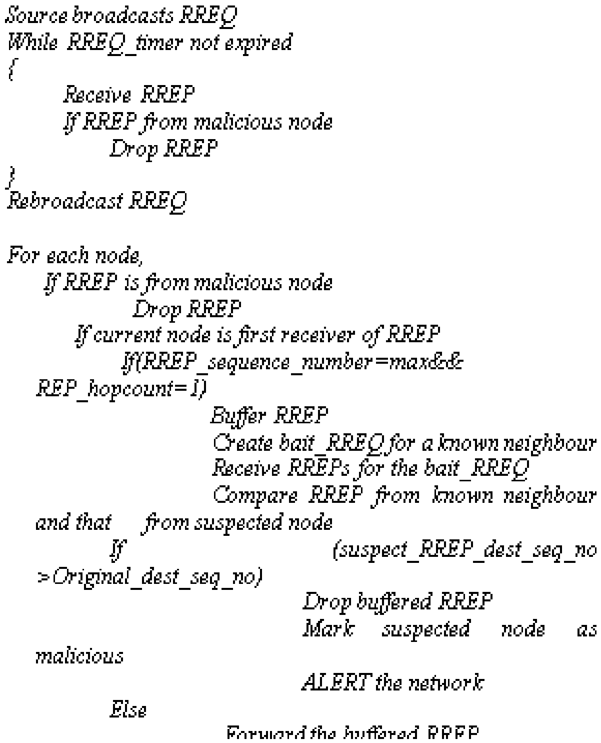


Fig 3: Secure Route Discovery

The second mechanism of the proposed scheme aims at detecting and isolating black hole nodes in the network. After performing the secure route discovery as shown in Figure 3, a route will be established between the source and destination. Two new parameters are added to the neighbour table of the node. The first parameter record the count of number of packets forwarded to the neighbour by the current node. The second parameter is used to count the number of packets overheard from the neighbour i.e., the count of packets further forwarded by the neighbour. Each time a data packet is forwarded by a node to its neighbour, it increments the forward count, *fvcount* for that neighbour in its neighbour table. A typical node is expected to forward the packets that are not destined for itself towards the actual destination. After forwarding the data packet, the node overhears the transmission of the neighbour to ensure whether the given packet is being correctly forwarded by that neighbour. If so, the node will increment the overhear count, *ovcount* for the neighbour.

In each interval, a node accumulates the number of *dropcount* for each of its neighbours. *Dropcount* for a neighbour is defined as the difference of packets forwarded to that neighbour and those forwarded by the neighbour. In normal circumstances, the *dropcount* will be low for a genuine node whereas it will be high for a malicious node. In each interval, when the *dropcount* for a node exceeds the threshold, the node is considered as malicious. Upon detecting such node, an alert packet is sent to alert the network. On receiving the alert packet, each node will update the id of the malicious node into to its malicious table. Subsequently, routes that pass through the malicious node are removed from the routing table. Also, all future messages from malicious nodes are discarded and not processed. Figure 5 illustrates the pseudocode of the second proposed mechanism.



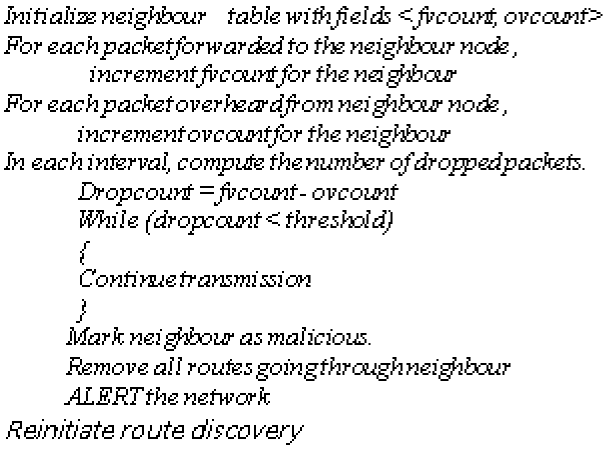
```
Source broadcasts RREQ
While  RREQ_timer not expired
{
        Receive  RREP
        If RREP from malicious node
              Drop RREP
}
Rebroadcast RREQ

For each node,
     If RREP is from malicious node
                Drop RREP
         If current node is first receiver of RREP
               If(RREP_sequence_number=max&&
    REP_hopcount=1)
                          Buffer RREP
                          Create bait_RREQ for a known neighbour
                          Receive RREPs for the bait_RREQ
                          Compare  RREP  from  known  neighbour
    and that     from suspected node
              If                       (suspect_RREP_dest_seq_no
    >Original_dest_seq_no)
                                  Drop buffered RREP
                                  Mark    suspected    node    as
    malicious
                                  ALERT the network
              Else
                              Forward the buffered RREP
```

Fig 4: Secure route discovery algorithm

5.1 Security Analysis

The first phase of the proposed algorithm secures the route discovery phase of the AODV protocol from black hole nodes. Instead of forwarding the received RREQ, each intermediate node checks the RREPs for suspicious routing information. If the reply is suspicious, additional checks are performed to confirm whether the reply is genuine. By rapidly detecting and isolating the black hole nodes in the route discovery phase itself, the number of packets dropped can be substantially reduced.

The second phase of the algorithm requires each node to keep track of the packets sent to its neighbours for further forwarding. Based on the packets received and forwarded by a node, the number of packets dropped by the node is computed. A node for which the drop count exceeds a drop threshold is treated as malicious and subsequently isolated from the network. By propagating the information about the malicious node in the network, further interaction with such node can be avoided and adverse effect on the network can be minimised. Thus, the algorithm can effectively prevent black hole nodes from affecting the performance of the network. In the proposed scheme, the packet delivery ratio (PDR) and throughput of the network is expected to be considerably improved.



```
Initialize neighbour    table with fields <fwcount, ovcount>
For each packet forwarded to the neighbour node ,
        increment fwcount for the neighbour
For each packet overheard from neighbour node ,
       increment ovcount for the neighbour
In each interval, compute the number of dropped packets.
       Dropcount = fwcount - ovcount
       While (dropcount < threshold)
       {
       Continue transmission
       }
      Mark neighbour as malicious.
      Remove all routes going through neighbour
      ALERT the network
Reinitiate route discovery
```

Fig 5: Packet flow monitoring algorithm

6. Conclusion

A method to counter black hole nodes in an on-demand routing protocol is proposed. The AODV algorithm is chosen as the base protocol on which the proposed solution will be implemented. The choice of AODV is due to the fact it is the most well-known on demand routing protocol. It also possesses the vulnerability in which a black hole node can exploit. In short, a secure route discovery is performed prior to actual data transmission. The typical behaviour exhibited by black hole nodes is exploited to distinguish between genuine and fake route replies. Experiments will be conducted to determine the effectiveness of the proposed algorithm and whether nodes that generate suspicious replies can be rapidly identified. Multiple black hole nodes can be detected using the proposed scheme. The second phase of the solution works by monitoring the data forwarding activities of a node. Any node with *dropcount* that exceeds the threshold is considered as malicious. The *dropcount* is a measure of number of packets received by a node and that are correctly forwarded by the node. Any node that detects the attacker alerts the entire network so that routes through the malicious nodes can be avoided in future.

References

[1] Neelam Khemariya and Ajay Khuntetha, "An Efficient Algorithm for Detection of Blackhole Attack in AODV based MANETs" International Journal of Computer Applications, Vol. 6, No.18, March 2013.

[2] Lalit Himral, Vishal Vig, and Nagesh Chand, "Preventing AODV Routing Protocol from Black Hole Attack" International Journal of Engineering Science and Technology (IJEST), Vol 3, July 2012.

[3] Niranjan Kumar Ray and Ashok Kumar Turuk, "Performance Evaluation of Different Wireless Ad Hoc Routing Protocols" International Journal of Wireless & Mobile Networks (IJWMN) Vol. 4, No. 2, April 2012.

[4] Maryam Gharooni, Mazdak Zamani, and Mehdi Mansourizadeh "A Confidential RFID Model to Prevent Unauthorized Access" 3rd International Conference on Information Science and Engineering (ICISE2011), September 2011. Yangzhou, China.

[5] K. Lakshmi, S.Manju Priya, A.Jeevarathinam K.Rama, and K.Thilagam, "Modified AODV Protocol against Blackhole Attacks in MANET" International Journal of Engineering and Technology, Vol. 2, pp. 444-449, 2010.

[6] Mehdi Medadian, and Khossro Fardad, "Proposing a Method to Detect Black Hole Attacks in AODV Routing Protocol" European Journal of Scientific Research, Vol.69 No.1, pp.91-101, 2012.

[7] S. Tamilarasan, "Securing AODV Routing Protocol from Black Hole Attack", International Journal of Computer Science and Telecommunications, Vol. 3, July 2012.

[8] M. Zaveri, N. Mistry, and D. C. Jinwala, "Improving AODV protocol against blackhole attacks" International Multi Conference of Engineers and Computer Scientists, IMECS, 2010.

[9] Govind Sharma and Manish Gupta, "Black Hole Detection in MANET Using AODV Routing Protocol" International Journal of Soft Computing and Engineering (IJSCE), Vol.2, April 2012.

[10] Ian D. Chakeres and Elizabeth M. Belding-Royer, "AODV Routing Protocol Implementation Design" 24th International Conference on Distributed Computing Systems Workshops, 2004.

Ayanwuyi Kolade is currently a M.S student within the Department of Information Technology at the Universiti of Kuala Lumpur, Malaysia. He received his B.Sc. degree in Information Technology from Kuala Lumpur Metropolitan University, Kuala Lumpur, Malaysia in 2011. His research interests Include computer networks, wireless and mobile ad hoc communications.

Megat F. Zuhairi is a Senior Lecturer within the System and Network Section in Malaysian Institute of Information Technology, Universiti Kuala Lumpur. He received his PhD in Electronics and Electrical Engineering from the University of Strathclyde in 2012 and M.S in Communication Networks and Software from the University of Surrey, UK in 2002. He is a currently an active researcher and a certified Cisco Network Academy Instructor in the institute. His research interests include computer data networking, and wireless mobile ad hoc communications.

Hassan Dao received the Ph.D. in engineering, 2013, the M.S. Computer and Information engineering in 2007 from International Islamic university Malaysia. He received Bachelor of Computer engineering from Sripatum university, Thailand in 2002. He is currently a senior lecturer within Computer engineering section at Universiti Kuala Lumpur, Malaysia. His research interests include signal processing communication, image processing, radio link design, RF propagation measurement, and wireless communication.

Sohail Khan is currently a Senior Lecturer within the Department of Computer Engineering at Malaysian Institute of Information Technology, Universiti Kuala Lumpur, Malaysia. He received his Ph.D. in Information and Systems Security from the Universiti Kuala Lumpur, Malaysia in 2014. Prior to this, he received his M.S. in Information Technology from the National University of Sciences & Technology, Islamabad, Pakistan in 2010 and B.S. in Information Technology from Institute of Business Management and Computer Sciences, Peshawar, Pakistan in 2005. His research interest includes trust management and security on modern smartphones, mobile malware analysis, security in Big Data and Internet-of-things (IoT). He has authored and co-authored many research papers in journals and conferences of international repute including ACM, Springer, IEEE, and Wiley Security and Communication Networks.