Design and Simulation of a Secured Routing Protocol for Mobile Ad-Hoc Network

Ibrahim K. Ogundoyin[1], Lawrence O. Omotosho[2], Kudirat O. Jimoh[3] and Adeyemi G. Yusuf[4]
[1,2,3,4]Department of Information and Communication Technology
Osun State University, Osogbo, Nigeria.
[1]ibraheem.ogundoyin@uniosun.edu.ng

Abstract
Mobile Ad-hoc Networks (MANET) consist of mobile nodes capable of performing self-configuration, communicate wirelessly with no centralized control and require routing protocols for its operation. However, the existing routing protocols used in MANETs are not secured and faced many security challenges which degrade the performance of the network. Therefore, there is need to build security feature in the existing routing protocol to enhance its performance in the face of emerging threats. In this paper, a proposed model was formulated to provide secure routing in MANET. The model used Public key cryptography also known as RSA with MD5 for authentication and observation-based cooperation enforcement and graph theory-based trust and reputation techniques, built on AODV routing protocol to enhance its security. The simulation of the model was carried out in NS2.35. Performance evaluation of the proposed model AODVRM was carried out by comparing its performance with an existing protocol, AODV using metrics like throughput, End-to-End delay and Packet delivery ratio. Simulation result showed that the proposed AODVRM recorded throughput of 291,502,502,461,506 kilo bytes per seconds (kbps), packet delivery ratio of 94%, 95%, 95%, 86%, 83% and an end-to-end delay of 132, 235, 272, 272, 258 seconds. While AODV recorded throughput of 280, 319, 227, 223, 74 kilo bytes per seconds (kbps). packet delivery ratio of 94%, 93%, 90%, 82%, 65% and an end-to-end delay of 186, 369, 341, 292, 278 seconds. In conclusion, the proposed model AODVRM is more efficient and performs better in the presence of attacks than the conventional AODV in terms of performance metrics used.

Keywords: MANET, Route, AODV, Algorithm, Performance, Simulation.

Introduction

Mobile ad hoc networks (MANETs) is an autonomous collection of mobile users without fixed infrastructure (Alem and Xuan, 2010; Adwan and Mahmoud, 2018] Sanzgiri *et al.*, 2002). Mobile ad-hoc networks (MANETs) are independent and non-centralized wireless connection of nodes. MANETs involve mobile nodes which are free in moving in and out in the network. Nodes are the devices like cell phone, laptop computer, individual electronic devices, MP3 player, and PC that form the mobile network. The nodes can function like a host, router or both at the similar time. They can form different topologies based on their connection with each other in the network. The nodes in MANET have self-configuration capability so they can be implemented quickly without the need for any infrastructure (Lu *et al*., 2009). However, wireless network like MANET is quite insecure due to the fact that wireless communication channels are unguided. Specifically, they are prone to eavesdropping and vulnerable to jamming, identity-based attacks, address spoofing, and Sybil attacks (Adwan and Mahmoud, 2018; Marepalli and Nagabhushana, 2008). Additionally, node mobility and resource constrain on mobile devices create significant challenges in detecting such attacks that have detrimental impact on network operations. Therefore, securing MANET is crucial to reliable operation and wide spread deployment of cyber–physical systems.There are existing routing protocols that determine how nodes in MANET communicate with each other and how to select routes between any two nodes on the network. Some of these protocols include: AODV, OLSR, DSR, etc. (Lu *et al*., 2009).

AODV is one of the well-known On-Demand Routing techniques (Patel and Jhaveri, 2016; Gupta *et al*., 2010). AODV protocol is prone and unprotected against so many attacks, namely; black hole, wormhole, jellyfish, gray hole, flooding and impersonation attacks. However, there have been research efforts to mitigate these attacks in MANET through enhancement of routing protocols. Some of the methods used in the course of research efforts to secure routing protocol include: RSA algorithm, RSA Digital Signature, CA distribution, Trust based threshold revocation method and identity (ID) based method (Gagan and Pallavi, 2013; Spinder and Harpreet, 2015; Banoth and Narsimha, 2016; Karamjeet and Chakshu, 2014; Marepalli and Nagabhushana, 2019; Waleed and Uttam, 2014). Unfortunately, the results and products from previously conducted research have not addressed the security challenges of the existing AODV completely as emerging threats are discovered in MANET on daily basis. Therefore, there is need to further enhance AODV in terms of security of information transmitted and

determining reputed routes for data transmission to avoid likely data interception in the network. This was achieved through the formulation of a secured protocol, AODVRM using techniques like MD5, RSA to secure information transmitted in the network, and the use graph-based trust model for determining reputation of route for data transmission in the network. The rest of the paper is organized as follows: review of related literature is presented in section 2. Section 3 presented the research methodology, description of the proposed model and algorithms. Section 4 presented simulation results and discussion, while conclusion is in section 5.

Literature Reviews

There are quite a good number of works regarding the state- of- the- art, secured routing protocol in MANET. Gagan and Pallavi (2013) proposed data transmission by using RSA algorithm for authentication purpose and a blacklist to prevent sending data packets to those nodes that are malicious. The proposed algorithm was more secured as compared to normal AODV routing algorithm. The performance was also analysed on different performance metrics using the NS2 simulator. The challenge with this proposed method is that it can only detect byzantine attack. In the same manner Spinder and Harpreet (2015) implemented RSA Digital Signature on AODV protocol and then compare the performance with RSA algorithm that is implemented on AODV protocol. The result showed that the energy consumed by RSA Cryptosystem is less as compared to RSA digital signature. This means that there is a need to reduce the complexity of the algorithm and save the energy of mobile nodes. Similarly, Mohammed and Sofiane (2017) proposed an enhanced approach based on first-hand reputation to detect misbehaved node in MANET. The approach comprises of three-phase which are monitoring, calculating reputation value and node isolation. The reputation value is enhanced by the packet dropped due to other events such as overloading of queue and node availability. The node with a negative reputation will be isolated, and an alert packet will be distributed to neighboring nodes. The simulation results showed that the proposed approach can detect and isolate a malicious node, which improved the packet delivery ratio and throughput but the approach is only limited to detecting misbehavior among nodes in MANET.

Banoth and Narsimha (2016) proposed a CA distribution and a Trust based threshold revocation method. In the work, the authors explained that many trust establishment solutions in MANET rely on public key certificates. Therefore, they should be accompanied by an efficient mechanism for proper certificate revocation and validation. The certificate authorities distribute the secret key to all the nodes. Followed by this, a trust-based threshold revocation method was computed which allows the misbehaving nodes to be eliminated. The performance analysis showed that this method can only eliminate misbehaving node. Waleed and Uttam (2014) presented an identity (ID) based protocol that secures AODV and TCP so that it can be used in dynamic and attack prone environments of mobile ad hoc networks. The proposed protocol protects AODV using Sequential Aggregate Signatures (SAS) based on RSA. It also generates a session key for each pair of source-destination nodes of a MANET for securing the end-to-end transmitted data. Here each node has an ID which is evaluated from its public key and the messages that are sent are authenticated with a signature/MAC. The proposed scheme does not allow a node to change its ID throughout the network lifetime. Thus, it makes the network secure against attacks that target AODV and TCP in MANET. When the performance analysis is taken, it showed that the proposed protocol is secured against attacks that are associated with AODV and TCP in MANET.

Masroor *et al.* (2018) proposed a framework that detected the selective forwarding attacks and computed the harmful host residing in an ad-hoc structure. The solution was further split into two phases: initial phase is the detection of selective forwarding attacks and the second phase performed the identification of malicious nodes. Performance of the proposed model was evaluated based on the network throughput, which was for the enhancement of security. Simulation of the proposed model was performed using Net Logo and the results showed an improvement of 20% in throughput of the network.

Sunilkumar *et al.* (2010) proposed a scheme called 2ACK which detected and mitigate routing behaviors. The scheme was based on simple 2-hop acknowledgment packet that is sent back by the

receiver of the next-hop link. The 2ACK transmission takes place for only a fraction of data packets, but not for all. The researcher embedded some security aspects with 2ACK to check confidentiality of the message by verifying the original hash code with the hash code generated at the destination. If 2ACK is not received within the wait time or the hash code of the message is changed then the node to next hop link of sender is declared as the misbehaving link. After the simulation was done, the result showed that the misbehavior in MANET was mitigated but the problem was that the 2ACK scheme only worked for detecting misbehavior.

Patel and Jhaveri (2016) proposed a method that combined the route discovery phase and the data transmission phase to detect malicious node. In route discovery phase, if the sequence number of destinations exceeds a threshold value then the RREP will be rejected. Then during the data transmission phase, the node calculates the difference between transmitted and received packets. If this difference exceeds a threshold value, then the node is malicious. The identities of malicious node are distributed to neighboring node and a blacklist is maintained.

Lu *et al.* (2009) proposed a protocol called SAODV after working with AODV and discovering that it is not secure enough. The researcher explained that the secured AODV prevent any security threat in which a node receives data and then drop it instead of forwarding it. The SAODV uses the hash chain algorithm to better secure AODV and then calls it SAODV. Performance analyses performed on SAODV showed that the rate at which packets were dropped by nodes on the network was low compared to AODV. The author did not consider packet delivery ratio and throughput as performance metrics.

Adwan and Mahmoud (2018) proposed a lightweight technique that uses timers and baiting in order to detect and isolate single and cooperative black-hole attacks in MANET. This technique was implemented on AODV routing protocol. The implementation of the proposed technique is performed by using NS-2.35 simulation tools. Simulation results of the proposed technique in terms of Throughput, End-to-End Delay, and Packet Delivery Ratio are very close to the native AODV without black holes. The proposed technique is only limited to detecting and isolating of single and cooperative black-hole attack.

Marepalli and Nagabhushana (2008) proposed a technique called (SDPEGH) which is used to secure, detect, prevent and eliminate Gray Hole. The authors explained that MANET are exposed to various security assaults especially gray hole, and in gray hole attack, selective dropping of packets arises, and the packet is unable to transmit further. Therefore, the Secure Detection Prevention and Elimination Gray Hole (SDPEGH) technique is considered the best method to solve the problem. In this study, DSDV routing protocol was considered and the recommended technique is implemented in NS-2 software. Performance evaluation of the proposed technique in terms of Throughput, End-to-End Delay, and Packet Delivery Ratio were analyzed and the result showed that the Secure Detection Prevention and Elimination Gray Hole (SDPEGH) technique worked effectively. The problem with the proposed technique is its limitation to gray hole.

The above reviewed literatures have contributed in no small measure to secure routing protocol in MANET. However, none of the contribution has achieved 100% efficiency as there are still compromises as a result of emergent threats. Therefore, there is a need to do more, by extending frontier of knowledge in this area of research and develop an improved security model for routing in MANET.

Methodology

The proposed system was modelled using RSA, MD5, observation-based cooperation enforcement and graph theory-based trust and reputation techniques, built on AODV routing protocol. RSA generates a private key and a public key for each node in the network. The keys are assigned to each node from source to destination. The RSA made the proposed model to output the private key and its corresponding public key as used in (Spinder and Harpreet, 2015). The MD5 message-digest algorithm is a widely used cryptographic hash function producing a 128-bit (16-byte) hash value, typically expressed in text format as a 32-digit hexadecimal number. MD5 accepts a message of any size as

input, and produces as output, a fixed-length message digest also known as signature (Fashoto *et al.*, 2010).

The Proposed Protocol Description

The proposed protocol model formulation assumed that nodes in MANET can be made to cooperate, thereby efficiently, reliably and securely route packets in the network. The proposed model has five phases described as follows:

Route Request Phase:

The source node broadcast route request message (RREQ) to its neighbor in order to find a route to the destination node. Each neighbor of the source node forwards the RREQ to their neighbor and so on until the destination node is reached. The destination node in turn send a route reply message (RREP) for each RREQ packet it received as shown in Figures 1 and 2.Each intermediate node receiving the RREQ update its routing table for the next-hop RREP and then send the PREP in the reverse-part using the store previous-hop node information. This process is repeated until the PREP reaches the source node.

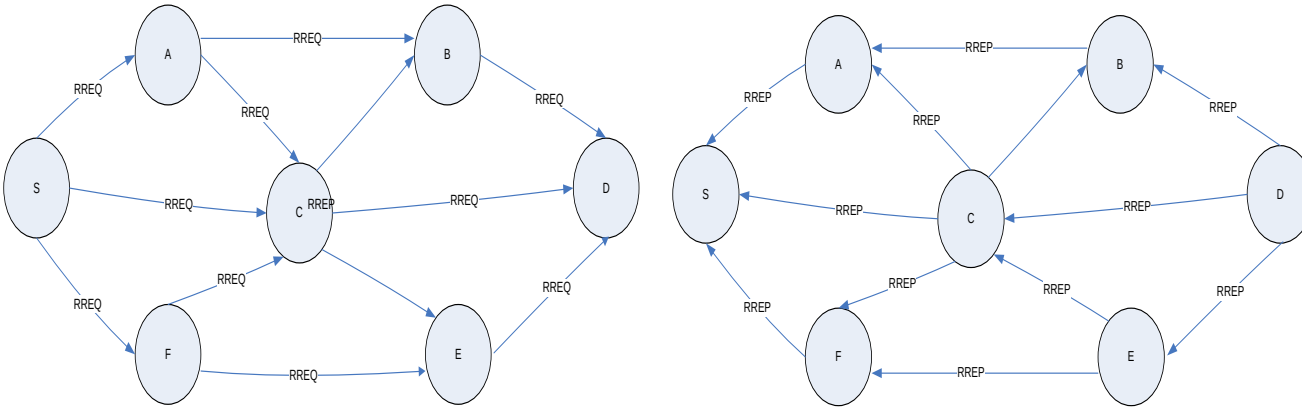

Figure 1: Route Request and Reply Phase

The Route Monitoring Phase:

Each node forwards a packet through the high reputed path. Route monitoring occurs based on the method designed for nodes in the MANET to forward their packets. The Source node creates an input message (M) and computes its message digest (sMD) using MD5 message digest algorithm as used in (citation). The source node also uses its private key in RSA to further encrypt message digest to get (esMD). The encrypted message digest (esMD) is attached to the input message (M) and the whole message (M, esMD) is sent to Destination. The destination gets the message (M, esMD) and extracts the encrypted message digest (esMD). It then computes its own message digest (dMD) of the received message (M). It also decodes received message digest (esMD) with source's public key provided by RSA and gets decoded message digest (desMD). The destination node then compares both message digest (dMD==desMD). Intermediate nodes between source and destination also perform this check. When both message digests matched, i.e. dMD and desMD, it means the message was not modified during the data transmission. But if both message digests are mismatched, it means the message was modified during the data transmission. With this process, misbehavior among nodes in the MANET is monitored; node which performs modification is identified by the next hop node, tagged it as attacker node and report to the source node to shut down the path and renegotiate a fresh or new route. Route monitoring is actually done by all the nodes in the MANET at any particular point in time as result of route monitoring mechanisms built into them. Figure 2 is an algorithm showing route monitoring phase of the MANET. If the number of dropped packets as a result of a node modification exceeds a threshold, it is considered as a selfish node and a notification is sent to the source node.

Route Monitoring Algorithm
{
Source node create an input message, M
// Source node call MD5 and RSA to compute message digest M and encrypt message digest, sMD respectively
sMD = MD5 (M) // message digest called as function
esMD = RSA (sMD) // function call RSA
// Source node send both esMD and M together to the destination through intermediate nodes
M-esMD = sNodeSendPacket (esMD, M)
// Both Intermediate and Destination nodes receive and decode M-esMD to detect modification of packets and node misbehaviours
(esMD, M) = dNodeReceivePacket (M-esMD)
dMD = MD5(M) // destination computes its own message digest dMD
Destination node uses public key to decodes the received message digest (esMD) from the source to get message digest (desMD)
//Destination node makes comparison
If
{
dMD==desMD
msg = "message was not modified during the data transmission, and no misbehavior"
}
Else
{
Msg = "message was modified during the data transmission, and there is misbehavior"
}
Shut the path, renegotiate a new path
End.
}

Figure 2: Route Monitoring Algorithm

The Data Transfer Phase:

During data transfer phase, the source node sends packets to the destination node choosing the highly reputed next hop node. The next hop node chooses highly-reputed next hop node from the routing table and stores the information in its sent table as the path for their data transfer. This process continues until the data packet reaches the destination node. Once the data packet reaches the destination the destination nodes sends a data acknowledgement (DACK) packet to the source node. The DACK traverses the same route as the data packet, but in the reverse direction.

The Reputation Phase:

In this model, nodes get reputation in two ways: First, during route monitoring, when source node send data packets through intermediate nodes to the destination nodes. The source node applies message digest and also encrypt the message digest to prevent modification by a malicious nodes. All intermediate nodes that pass the sent message or packet without modification get reward by getting its reputation or trust value incremented. Second, because of sophistication of MANET threats as a result of emergence of new applications, calculating trust must be multilayered. Other threats may not be interested in modification but just want unnecessary disruption of the MANET to degrade its QoS. We therefore, introduce another layer of trust and reputation based on graph theory to determine a secured route during data transfer.

A Graph is an ordered pair , $G = (V, E)$

Comprising,

V is a set of *vertices* (also called *nodes* or *points*);

$E \subseteq \{\{x, y\} \mid (x, y,z,w,r,k, p) \in V^2 \wedge x \neq y\}$ a set of *edges* (also called *links* or *lines*), which are unordered pairs of vertices (i.e., an edge is associated with two distinct vertices). Figure 3 is an example of a typical graph.

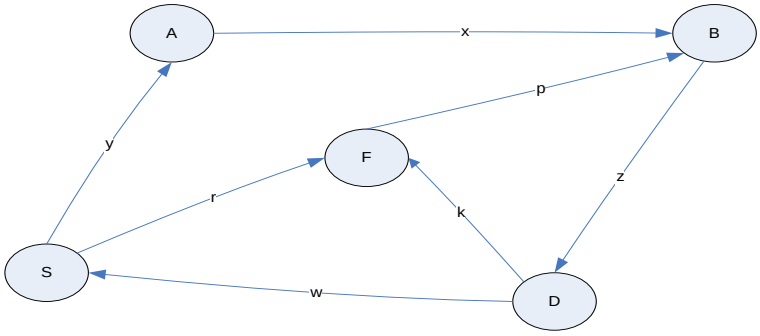

Figure 3: A Typical Graph

A graph can be directed and undirected. In a directed graph, all the edges are directed from one node to another while the edges of undirected graphs have no direction. In a directed graph, each node has in-degree and out degree. The in-degree of a node is the number of edges directed on a node, while the number of edges emanating from a node is the out-degree. This mathematical model was used to model trust and reputation through which secured route were determined in the proposed model. The assumption is that every node could receive and also send packets. The number of edges pointing to a node (in-degree) indicate the number of packets received by the node, while the number of edges originating (out-degree) from the node is the number of packets sent or forwarded by the node. When a source node sends packet to the destination, all intermediate nodes between the source and destination must have in-degree equal to the out-degree. This indicates that the number of packets sent through the intermediate nodes in the network is forwarded to the next-hop node. Any intermediate node that behaves contrary will have it trust value decremented by -1 otherwise incremented by +1.

The Shutdown Phase:

In the shutdown phase, nodes are demoted for misbehavior, selfish act or maliciousness. The proposed model also incorporated monitoring agent (MA). The MA watches and counts the in-degree and out-degree of intermediate nodes between source and destination. If at any point in time there is mismatch between in-degree and out-degree within a set period 5seconds within which the node is expected to forward the pack for the next hop node, the packet is suspected to misbehave, thereby have its trust value reduced by -1. If the set period of 5seconds is exceeded, it is termed malicious. The MA raises alarm and informs the source node for shutdown of the path and renegotiates a new path. Such node will have it trust value reduced by -2. If the trust or the reputation of the next hop node goes below the threshold of (-20), the current node deactivates this node in it routing table and send an error message RERR to upstream nodes in the route. Nodes whose reputation value reached (-40) is temporarily isolated from the MANET for five minute and latter join the network as a new node with a value of (0). The source node will have to reinitiate the route discovery process again. The algorithm for shutdown phase is as presented in figure 4. Figure 5 presents the step by step description of the various phases in the proposed protocol model.

Shutdown Phase Algorithm
{
Source node create an input message, M
Intialise in-degree, out-degree and set time counter
Monitoring Agent, MA set to active state
Source nodes send packet
Packets received by intermediate nodes
Calculate both in-degree and out-dergree of intermediate nodes
//Compare in-degree and out-degree
For node ith
Is in-degree ==out-degree
{
Node behaving well
Increment reputation by +2
}

```
Else
{
Is the set time for normal processing of 5s not exceeded?
        {
        Target node to be selfish
        Decrement reputation by -1 for the node
        }
        Else
        {
        Tag node as malicious
        Decrement reputation by -2
        MA to raise alarm, notify source node to shutdown the current path and initialize a fresh path
        }
}
}
```

Figure 4: *Shutdown Phase Algorithm*

```
//Proposed AODVRM Model
Get the source nodeX ready to send information to the Destination node
// Broadcast a route request through intermediate nodes between source and destination
 SendRREQ (nodeX)
{
SET Sqn#_rq =1, Hop_count_rq = 0
 BROADCAST RREQ to Neighbors
}
 ReceiveRREQ (RREQ, nodeX)
{
 IF (nodeX == Destination)
{
UPDATE Route, SendRREP (nodeX, RREQ)
IF (nodeX! = Destination)
{
Broadcast and do necessary update until it reaches the destination node
}
// Return Route reply RREP from Destination node
SendRREP(nodeX, RREQ)
{
SET Sqn#_rp = Seq#_rq, Hop_count_rp = 0
BROADCAST RREP to Neighbors
}
ReceiveRREP (RREP, nodeX)
 {IF (nodeX == Source) UPDATE Route, DATA
 IF (nodeX != Destination) {
Broadcast and do necessary update until it reaches the source node
}
// Source nodeX sending information after establishing route to the destination node
{
Source node inputs message, M
// Source node call MD5 and RSA to compute message digest M and encrypt message digest, sMD respectively
sMD = MD5 (M) // message digest called as function as used in
esMD = RSA (sMD) //  RSA called as function to encrypt message digest sMD
// Source node send both esMD and M together to the destination through intermediate nodes
 M-esMD = sNodeSendPacket (esMD, M)
// Both Intermediate and Destination nodes receive and decode M-esMD to detect modification of packets and
node misbehaviours
(esMD, M) = dNodeReceivePacket (M-esMD)
dMD = MD5(M) // destination computes its own message digest dMD by calling MD5 function
Destination node uses public key to decodes the received message digest (esMD) from the source to get message
digest (desMD)
//Destination node makes comparison
```

```
If
{
        dMD==desMD
msg = "message was not modified during the data transmission, and no misbehavior"
}
Else
{
Msg = "message was modified during the data transmission, and there is misbehavior"
}
Shut the path, renegotiate a new path
End.
}
```

Figure 5: Proposed protocol (AODVRM) Algorithm

Performance Evaluation of the Proposed Model

The proposed AODVRM was benchmarked with the existing AODV using metrics as described below:

Network Throughput

In MANET, network throughput is the average rate odf successful message delivery of a communication channel. These data may be delivered over a physical, logical or through a certain network node. It can be expressed as the ratio of the data packet delivery to the destination to those generated by the source in bit per second (bps), kilobyte per second (kbps) or megabyte per second (mbps). A high network throughput is desirable for any protocol. One factor that affects throughput in MANET is mobility. The higher the mobility, the lower the throughput. This is because a higher mobility leads to frequent topology changes which in turn affect data being sent to different destinations. Mathematically, throughput T is expressed using equation 1 as in (Gupta *et al.*, 2010).

$$T = \frac{1}{c}\sum_{f-1}^{c}\frac{R_f}{N_f} \quad (1)$$

Where, T is the network throughput, C is the total number of connection, f is the unique flow identifier R_f is the count of packet received, N_f is the count of packet transmitted.

End-to Delay

The average delay includes the end-to-end delay and media access delay. The end-to-end delay refers to the time taken for a packet to be transmitted across a network from source to destination, it includes all possible delays caused by buffering during rout discovery latency, queuing at the interface, queue propagation and transfer time. Different applications have different levels of tolerance delays. While an MTP application can tolerate delay up to a certain threshold, voice and video application require low delays to avoid jitters. End-to-end delays, therefore measures the effective reliability of a routing protocol. A strong factor here is a mobility of the nodes. A higher mobility rate leads to increase in delay. The average end-to-end delay D is defined in equation 2 in (Gupta *et al.*, 2010) as:

$$D = \frac{1}{N}\sum_{i-1}^{n}(r_i - s_i) \quad (2)$$

Where, D is the end-to-end delay measured in ms, N is the number of successfully received packet, I is the unique packet identifier, r_i is the time at which a packet with unique id i is received, s_i is the time at which a packet with unique ID i is sent. Media access delay is the time from when data reaches the MAC layer until it is successfully transmitted out on the wireless medium. The reason for studying average access delay is that many real-time applications have maximum tolerable delay, after which the data will be useless. Therefore, it is important to provide low delay for real-time flows.

Packet Delivery Ratio

PDR is the ratio of the packet sent from the sender to the packets delivered to the receiver.

Experimental Design and Simulation Environment

Simulation was setup for the proposed secured AODVRM protocol using NS 2.35 on Ubuntu Linux 18.04.2 desktop Operating System environment. The performance of the AODVRM was benchmarked

with the existing AODV protocol, simulation of AODV was done in (Gupta *et al.*, 2010). Each node on the proposed AODVRM protocol was configured to run MD5, RSA algorithms to secure data being transmitted. The nodes were also designed to have trust table and MA for handling malicious and selfish node misbehavior. The existing AODV protocol was configured in such a way that all connecting nodes communicate with the server for information. In a nutshell, the AODV was implemented as an office network using the configuration setting as shown in simulation setup setting presented in Table 1. The simulation was run on 20 nodes network for different simulation time scenarios. The mobile nodes and the server were spread randomly within the geographical area. The ad hoc routing protocol was set to AODV and TCP traffic was used to study the effects of the protocol. In the profile configuration, FTP application was deployed for the study and all other settings were left at default. The nodes were WLAN mobile client with a data rate set at 11 mbps and transmitting with 0.005 watts power. Random waypoint mobility model was used because it is a simple and widely accepted mobility model to depict more realistic mobility behavior. The nodes move at a constant speed of 10 m/s. The simulation was run for different chosen time.

The implementation of AODVRM protocol was carried out by modifying the AODV protocol configuration. The fixed WLAN server was modified to FTP server to serve as the destination node for the FTP application. On Each WLAN workstation advanced node model interface, four (4) processes were created: MD5, RSA, the trust table process and MA process. The MD5 produces message digest sMD of message M sent by a source node. Figure 6 is a screenshot of message digest of MD5 during one of the simulation scenarios. The RSA encrypts the message digest for further security of the information sent by the source node. Figure 7 is the snapshot of public key and private key generated for each Node. The encrypted message digest (esMD) was attached to the input message (M) and the whole message (M-esMD) was sent to Destination. In the course of transmission, the trust table process which was configured to store the trust reputation value was invoked to connect nodes having reputation in the network so as to create a secured route through which message sent could be securely delivered. The MA process configuration enables the current node to monitor the next hop on the network against selfish behavior. When the destination gets the message (M-esMD), it extracted the encrypted message digest (esMD) and computed its own message digest (dMD) of the received message (M). The source also decoded received message digest (esMD) with source's public key and gets decoded message digest (desMD). The destination then compared both message digest (dMD==desMD). At any simulation running scenario, when both message digests matched, it means the message was not modified during the data transmission. However, if both message digests are mismatch, it means the message was modified during the data transmission. The node with such modification will be identified and tagged as malicious node. Figure 8 is a screenshot showing malicious node detection during simulation. Figure 9 is a Snapshot of new secure route established after a malicious node was detected along a route.

Table 1: Parameter Settings for the Proposed protocol Simulation Environment

Simulation Tool	NS2.35
Operating System	Ubuntu Linux 18.04.2 desktop
Interface Queue Length	1500
Channel	Wireless Channel
Simulation Stops	6.0min
No. of Nodes	20
Mac	Mac/802_11
Antenna model	Antenna/Omni Antenna
Interface QueueType	Queue/Drop Tail/PriQueue
Link Layer Type	LL
Energy Model	Energy Model
Radio Model	Radio Model
Initial Energy	1000
Ad-hoc Routing	AODV
Simulation Area	1200M*1200M

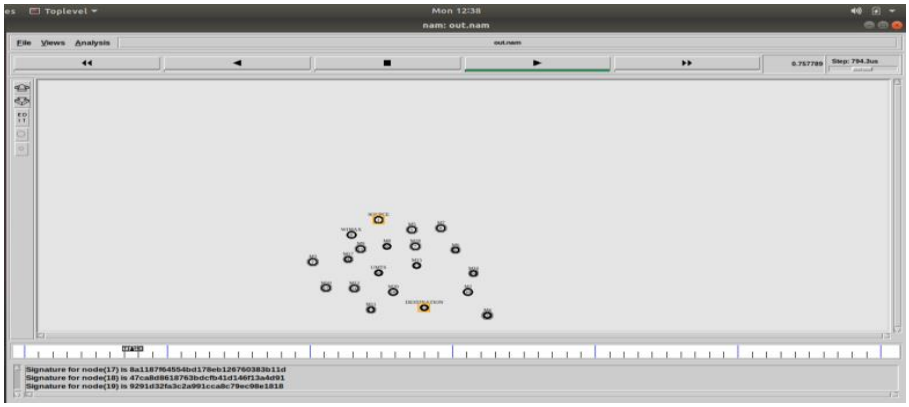

Figure 6: Snapshot of Signature of each Node

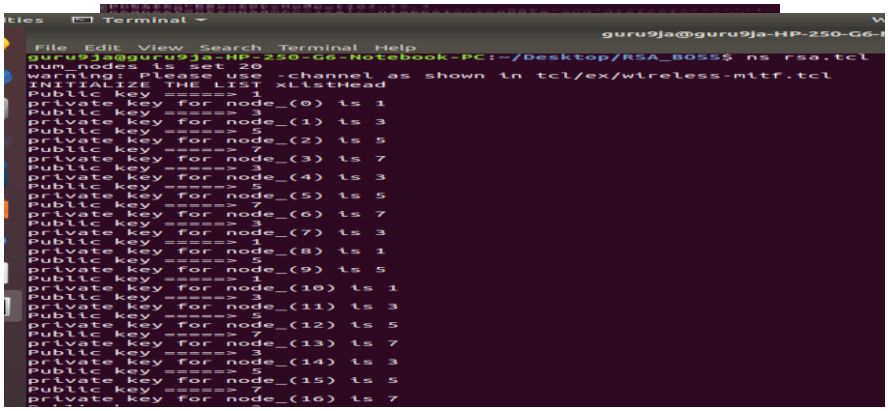

Figure 7: Snapshot of Public key & Private Key generated for each Node

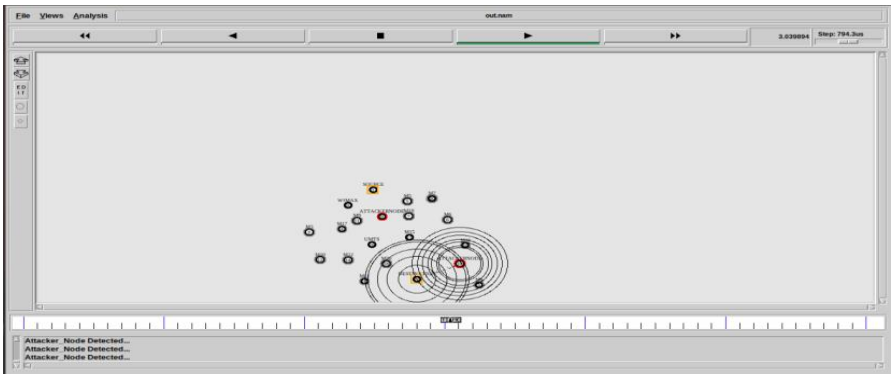

Figure 8: Attacker Node Detected

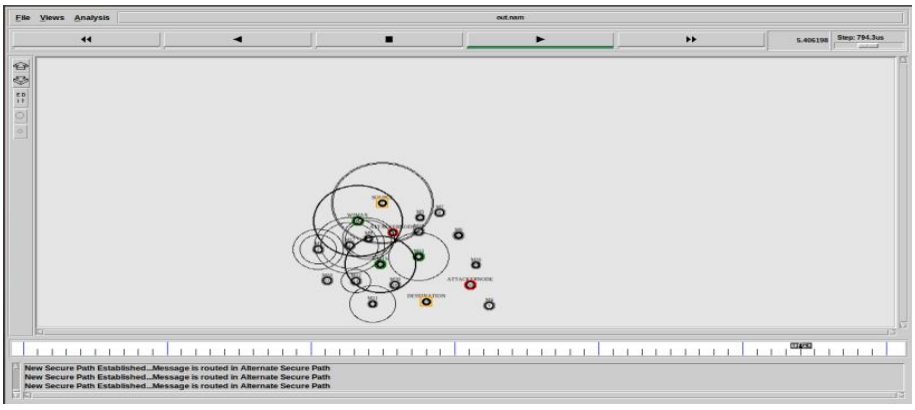

Figure 9: Snapshot of New Secure Route Established

Result and Discussion

In this study, the proposed AODVRM protocol performance was evaluated using the following performance metrics

The Throughput

Throughput is the ratio of total number of data packets that are delivered or received per unit simulation time. The higher the throughput, the better is the protocol. AODVRM recorded throughput of 291, 502, 502, 461, 506 kilo bytes per seconds (kbps) while AODV recorded throughput of 280, 319, 227, 223, 74 kilo bytes per seconds (kbps) as shown in Figure 10.

The Packet Delivery Ratio (PDR)

PDR is the ratio of the packet sent from the sender to the packets delivered to the receiver. Figure 11 shows that AODVRM recorded packet delivery ratio of 94%, 95%, 95%, 86%, 83% while AODV recorded packet delivery ratio of 94%, 93%, 90%, 82%, 65%. This is so because AODVRM protocol is secured and has a way to avoid malicious node and route in the network, hence the increased PDR.

The End to End Delay

The end to end delay signifies the time taken for message to be transmitted from the source to the destination. AODVRM recorded delay of 132, 235, 272, 272, 258 seconds while AODV recorded delay of 186, 369, 341, 292, 278 seconds as shown in Figure 12. The reason for this is that, AODVRM protocol is secured, using the protocol, it was easy to identify malicious node. Therefore, data transmission did not route thee malicious node unlike in the AODV protocol which is not secured. The malicious node was able to intercept some of the messages sent; this increased the delayed experience I the network.

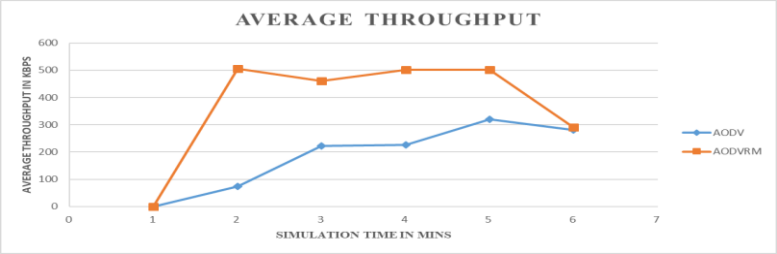

Figure 10: Graph Showing Throughput

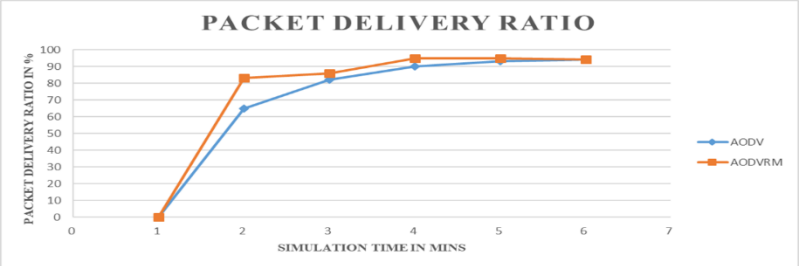

Figure 11: Graph Showing Packet Delivery Ratio

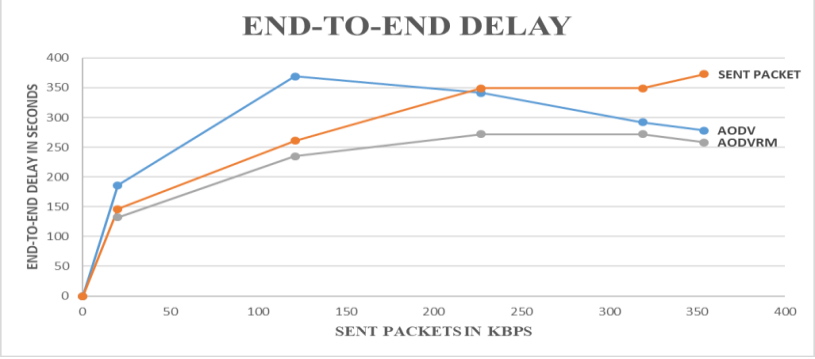

Figure 12: Graph Showing End-to-End Delay

Conclusions

In this research work, various security techniques to mitigate routing attacks on MANET were investigated. A secured routing protocol was modelled using RSA, MD5, observation-based cooperation enforcement and graph theory-based trust and reputation techniques, built on AODV routing protocol for MANET. The choice of RSA and MD5 used in the model formulation enable the proposed model to pace up with dynamism of emerging threats in MANET. The RSA was used to generate public key and private key while the MD5 was used to generate signature or message digest. The proposed model when simulated, its results were compared with conventional AODV in the face of attacks using metrics such as throughput, end-to-end delay and packet delivery ratio. The results showed that the proposed model, AODVRM in this research performed better in terms of the metrics used. We conclude that AODVRM is efficient, reliable and secured. The model will enhance MANET protection if adopted in place of conventional and available routing protocols.

References

Adwan Y. and Mahmoud A. Z. (2018) "Detecting and Isolating Black-Hole Attacks in MANET Using Timer Based Baited Technique", Hindawi Wireless Communications and Mobile Computing Journal, 18(10), 1-10

Alem Y.F. and Xuan Z.C. (2010) "Preventing Black Hole Attack in Mobile Ad-hoc Networks Using Anomaly Detection" 2nd International Conference on Future Computer and Communication (ICFCC 2010), 3, 672-676.

Banoth R. and Narsimha G. (2016) "Trust Based Certificate Revocation for Secure Routing in MANET", 2nd International Conference on Intelligent Computing, Communication & Convergence, 92, 431-441.

Fashoto S.G, Gbadeyan J.A and Okeyinka E.A (2010) "Application of Digital Signature for Securing Communication Using RSA Scheme based on MD5" Proceedings of the International Conference on Software Engineering and Intelligent Systems, July 5th-9th, Ota, Nigeria 1, 371-380.

Gagan S. and Pallavi K. (2013) "A Secure routing protocol for Mobile Ad Hoc Networks against byzantine attacks", Computer Networks & Communications (NetCom), Lecture Notes in Electrical Engineering, 2, 4614-4621.

Gupta, A.K., Sadawarti, H. and Verma. A.K. (2010) Performance Analysis of AODV, DSR and TORA Routing Protocols. International Journal of Engineering and Technology, 2(2), 226 - 231

Karamjeet S. and Chakshu G. (2014) "Using MD5 AND RSA Algorithm Improve Security in MANETs Systems", International Journal of Advances in Science and Technology, 2, 2348-2356.

Lu S., Li L., Lam K. and Jia L. (2009) "SAODV: a MANET routing protocol that can withstand black hole attack", International conference on computational intelligence and security, 2, 11-14.

Marepalli R. and Nagabhushana R. (2019) "Gray Hole Attack Detection Prevention and Elimination using Sdpegh in Manet", International Journal of Engineering and Advanced Technology (IJEAT), 8, 605-614

Marepalli and Nagabhushana (2008) "A localized certificate revocation scheme for mobile ad hoc networks," Ad Hoc Networks, 6(1),17-31.

Masroor A., Zahid U., Meharban K. and Abdul H. (2018) "Secure and Efficient Routing Mechanism in Mobile Ad-Hoc Networks", International Journal of Advanced Computer Science and Applications, 9(4), 436-441.

Mohammed A. and Sofiane B. (J2017) "An Enhanced Reputation-based for Detecting Misbehaving Nodes in MANET", I.J. Wireless and Microwave Technologies, 4, 28-37.

Patel A. and Jhaveri R. (2016) "Addressing Packet Forwarding Misbehavior with Two Phase Security Scheme for AODV-based MANETs", International Journal of Computer Network & Information Security, 5, 55-62.

Sanzgiri K., Dahill B., Levine B. N. and Shields C. (2002) "A Secure Routing Protocol for Ad Hoc Networks" in proc. of Network Protocols Proceedings. 10th IEEE International Conference, 78-87.

Spinder K. and Harpreet K. (2015) "Implementing RSA Algorithm in MANET and Comparison with RSA Digital Signature", International Journal for Advance Research in Engineering and Technology, 3(5), 24-28.

Sunilkumar M., Lokesh B., and Vittalkumar V. (2010) "Routing Misbehavior Detection in MANETs Using 2ACK", Journal of telecommunication and information technology, 4, 105-111.

Waleed S. and Uttam G. (2014) Secure Routing and Data Transmission in Mobile Ad Hoc Networks", International Journal of Computer Networks & Communications (IJCNC), 6(1),111-127.