Nigerian Journal of Technology (NIJOTECH)
Vol. 37, No. 2, April 2018, pp. **498 – 507**

Print ISSN: 0331-8443, Electronic ISSN: 2467-8821
www.nijotech.com
http://dx.doi.org/10.4314/njt.v37i2.28

RTDSR PROTOCOL FOR CHANNEL ATTACKS PREVENTION IN MOBILE AD HOC AMBIENT INTELLIGENCE HOME NETWORKS

S. A. Akinboro[1,*], E. A. Olajubu[2], I. K. Ogundoyin[3] and G. A. Aderounmu[4]

[1,] DEPT. OF COMPUTER SCIENCE AND TECHNOLOGY, BELLS UNIVERSITY OF TECHNOLOGY, OTA, OGUN STATE, NIGERIA
[2,4], DEPT. OF COMPUTER SCIENCE AND ENGINEERING, OBAFEMI AWOLOWO UNIV., ILE-IFE, OSUN STATE NIGERIA
[3,]DEPT. OF INFORMATION AND COMMUNICATIONS TECHNOLOGY, OSUN STATE UNIV., OSOGBO, OSUN STATE NIGERIA
E-mail addresses: [1] *akinboro2002@yahoo.com,* [2] *emmolajubu@oauife.edu.ng,* [3] *olaac@ymail.com,*
[4] *gaderoun@oauife.edu.ng*

ABSTRACT

In ambient intelligence home networks, attacks can be on the home devices or the communication channel. This paper focuses on the channel attacks prevention by proposing Real Time Dynamic Source Routing (RTDSR) protocol. The protocol adopted the observation based cooperation enforcement in ad hoc networks (oceans) and collaborative reputation mechanism built on Dynamic Source Routing (DSR) protocol. The RTDSR introduced lookup table on the source, destination and intermediate nodes. It also ensures that data path with high reputation are used for data routing and a monitoring watchdog was introduced to ensure that the next node forward the packet properly. The RTDSR protocol was simulated and benchmarked with DSR protocol considering network throughput, average delay, routing overhead and response time as performance metrics. Simulation result revealed a better performance of RTDSR protocol over existing DSR protocol.

Keywords: *RTDSR, Ambient, Home network, Channel attacks, Protocol, Packet, OPNET*

1. INTRODUCTION

Ambient Intelligence (AmI) is the capability of an environment, populated by electronic devices, to exhibit a certain degree of intelligence. To be perceived as intelligent, the whole environment must act in a smart way. It also requires that, each single component in the environment actively cooperates with the others so that the whole environment can remain coherent [1].

Communication among the electronic devices can be facilitated by mobile ad hoc network (MANET) or wireless networking [2]. MANET due to their improvised nature is frequently established in insecure environments and hence susceptible to attacks. MANET attacks can be classified into external or internal attacks. Solution to external attacks can be provided using the established wired networks methods such as firewall, because the attackers are not trusted nodes on the network. Internal attacks are more dangerous because compromised nodes are originally the first users of the MANET. They can easily pass the authentication and get protection from the security mechanism. The adversaries can make use of the malicious nodes to gain normal access to confidential services.

Routing protocols in MANET are the common target of these internal attackers. Therefore, Routing security solutions should be designed to focus on the internal attacks.

DSR have been proposed as a routing security solution because it is a simple and efficient routing protocol designed specifically for used in multi-hop wireless ad hoc networks [3]. It uses trust matrix table at the source node. All the intermediate and destination nodes communicate with the source node for update routing information which could cause delay on the network. The DSR could not provide cooperation capability among the nodes in the data path. This is necessary to ensure that no node will refuse forwarding packets to the next hop. This setback makes DSR protocol not suitable as a security routing solution for securing communication channel in ambient intelligent home.

This study therefore proposed a RTDSR protocol to protect the channel against malicious and selfish behaviour. In the RTDSR protocol, intermediate nodes have lookup table to store routing information and

***Corresponding author tel: +234 – 805 – 335 – 0677**

update the routing table promptly. Data path with high reputation are used for data routing. Monitoring watchdog was introduced to ensure that the next hop forward their packet properly. This could go a long way in protecting the lives in the AmI home against network disruptions which may result to loss of life.

The rest of the paper is organized as follows: review of related work is presented in section 2. Presented in section 3 are the proposed RTDSR protocol and performance evaluation for the RTDSR protocol. Section 4 presented the description of simulation environment, section 5 talks about simulation result and discussion, while conclusion is in section 6.

2. RELATED WORK

A review of literatures on MANET routing protocols development was done but none of them was adapted to ambient home network routing protocols that can provide efficient solution to malicious and selfish nodes attacks. A protocol to eliminate failure in MANET using strength parameter in AODV and provide a stable path for data transmission was proposed in [4]. Identification of broken link was done by using request and reply method which leads to less routing overhead and high packet delivery ratio. A new routing protocol in Cognitive Radio Ad hoc Network called Opportunistic Routing (CRCN CORMEN) was provided in [5]. The new protocol was used as an alternative to maximize the packet delivery ratio. The nodes work in cooperative manner among the neighboring nodes for transformation of packets from the source to destination. The ECLIDAR methodology for cross layer intrusion detection which identifies various attacks in MANET ws discussed in [6]. Data traces are collected from various layers using association, clustering algorithm. The ECLIDAR Algorithm was able to detect both known and unknown attacks, and adaptive response action was provided based on the severity of the attacks. |Broadcast storm in MANET using adaptive information dissemination (AID) algorithm was reduced by [7]. Each node can dynamically adjust the values of its local parameters using information from neighboring nodes. The dynamic adjustment does not require any additional effort such as distance measurements or exact location determination of nodes. Cooperative MAC protocol called EAP – CMAC (Energy Aware Physical – Layer Network Coding Cooperative MAC) was introduced in [8]. The protocol integrates cooperative communication into PNC in wireless ad hoc networks. EAP – CMAC selects the best transmission mode among direct transmission traditional cooperation and PNC – based transmission, by considering the destination queue and source – destination link quality. A reputation based dynamic source routing (RDSR) protocol was proposed in [9]. The source node sends packets to only the hop with high reputation value and this is repeated by next hop neighbours until the packet reach the destination. The model has fewer message overhead and very high reliability when the nodes misbehaved. A trust model to secure the network and stimulate cooperation by excluding misbehaving nodes from the network was proposed in [10]. Local and global trust scheme, exclusion mechanism and voting scheme for malicious node punishment was used. The problem of mobile malicious node attacks, and description of the limitations of various naive measures that might be used to stop them was identified in [11]. To overcome these limitations, they propose a scheme for distributed detection of mobile malicious node attacks in static sensor networks. The scheme applied sequential hypothesis testing to discover nodes that are silent for unusually many time periods. Through analysis and simulation, the proposed scheme achieves fast, effective, and robust mobile malicious node detection capability with reasonable overhead. Direct trust evaluation using the features of the node and fuzzy logic to model the node, the network and the environment was proposed in [12]. Fuzzy trusted dynamic source routing (FTDSR, FTDSR-1 and FTDSR-2) protocol was used to make multiple stage decision. Security decision on data protection, secure routing and other network activities for ad hoc network. The model captures attack effectively was provided in [13]. The protocol achieves average security level based on knowledge, experience accumulation and inference. The security solution is subjected to delay due to the trust matrix table at the source node. This made the solution not suitable for environment where security threat is very high. Also, an approach for the detection of single and collaborative black hole attacks in MANET with reduced computational and routing overhead was proposed in [13]. This method makes use of a fake RREQ (route request) with nonexistent target address, destination sequence number and next hop information extracted from RREP (route reply) to identify the malicious nodes. A mechanism for preventing warm hole attack in Ad Hoc Network using AODV protocol where communication between nodes takes place through IP address was proposed in [13]. When a source node wants to send message to the destination node, a secure path is created that contains IP address and sequence. Presence of malicious node between the created paths is identified because malicious node does not have its own sequence number. A trust-based full fledge secure communication in vulnerable MANET using non-cryptographic mechanism was proposed in [15]. The model performs efficient management of

authentication key depending on trust and collective based schema. This secure mechanism can perform better in a high scale network with higher mobility than cryptographic based technique.

Performance analysis of some MANET routing protocol was carried out such as; [16], which compared Ad hoc On-Demand Distance Vector (AODV), Dynamic Source Routing (DSR) and Destination Sequence Distance Vector (DSDV). AODV and DSR are superior to the DSDV. DSR outperforms AODV in less stressful situation while AODV outperforms DSR in more stressful situation. In [17], trust scheme that observed the behaviour of mobile nodes such as node mobility was proposed. The scheme avoid communication through these nodes to enhance routing security. In [18], the effect of black hole attack on AODV and improved AODV was analyzed. The vulnerability of the two protocols was analyzed under varying pause time. The overhead of AODV was twice compared to improved AODV, also the effect of malicious node on IAODV was less.

We observed to the best of our knowledge, that no literature has proposed a secure routing solution for ambient intelligent home network and if there is any, they need to be strengthened because of emerging threats. Also the cooperation of nodes in MANET network is very important because lack of cooperation could result to selfish behaviour and may eventually lead to denial of service attacks. Most ad hoc routing protocols such as AODV and DSR were not originally designed to be secured against malicious attacks as they rely on implicit trust your neighbour relationship [17].

Hence the needs for this research work, to develop a secure routing solution for ambient intelligent home network. The routing solution will prevent selfish and malicious behavior on the MANET channel.

3. PROPOSED REAL TIME DYNAMIC SOURCE ROUTING (RTDSR) PROTOCOL

The AmI home network was provided by MANET. The attacks on the communication channel could be denial of service which includes flooding, jamming and eavesdropping [19], selfish behaviour etc. The proposed RTDSR protocol uses the idea of observation based cooperation enforcement in ad hoc network protocol and collaborative reputation mechanism built on dynamic source routing (DSR) protocol. The protocol assumed that the ad hoc nodes can authenticate with each other correctly and was described with five phases namely:

Route discovery phase: The source node broadcast route discovery message (RDM) to its neighbours in order to find a route to the destination node. Each neighbour of the source node forward the request to their neighbours and so on until the destination node is reached. The destination node uncast a route reply confirmatory message (RRCM) for each RDM packet it received as shown in Figures 1 and 2. Each intermediate node receiving the RRCM updates its routing table for the next-hop RRCM and then unicast this RRCM in the reverse-path using the stored previous-hop node information. This process is repeated until the RRCM reaches the source node.

The route monitoring phase: Each node forwards a packet through the high reputed path. A watchdog mechanism on the node in Figure 3, monitors the next node behaviour and confirm that it forward the packet properly. The watchdog determines misbehaviour by coping packets to be forwarded into a buffer and monitor the behaviour of the adjacent node to these packets. It promiscuously snoops to decide if adjacent node forwards the packets without modification. If the packets that are snooped match with the observing node's buffer, then they are discarded, whereas packets that stays in the buffer beyond a timeout period without any successful match are flagged as having been dropped or modified. If the number of dropped packets by a node exceeds a threshold, it is considered as a selfish node and a notification is sent to the source node.

The data transfer phase: The source node sends packets to the destination node chosen the highly reputed next hop node as shown in Figure 4. The source node will start a timer before it receives a data acknowledgement from the destination. Thereafter the chosen next hop node will choose the highly-reputed next hop node from its routing table and will store 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 its destination, the destination node sends a signed 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: An intermediate node receives a data acknowledgement packet. It retrieves the record stored during the data transfer that correspond to this data packet and then increment the reputation of the next hop node. Also it will delete the data entry from its sent-table. Once the DACK packet reaches source node, it deletes the entry from its sent table and gives a recommendation of (+1) to the node that delivered the acknowledgement.

The timeout phase: If the timer for a given data packet expires at a node, the node retrieves the entry corresponding to the data transfer operation returned by the timer from its sent-table. Then the node gives a

negative recommendation (-2) to the next-hop node and delete the entry from the sent-table. When the intermediate nodes timers up to the node that dropped the packet expire, they give a negative recommendation to their next hop node and delete the entry from their sent table. All the nodes between the misbehaving node and the sender, including the misbehaving node get a recommendation of (-2). If the reputation of the next-hop node goes below the threshold of (-40), the current node deactivates this node in its routing table and send an error message RERR to the upstream node in the route. Nodes whose reputation value reached (-40) is temporarily isolated from the MANET for five minutes and later join the network as a new node with a value of (0). The source node will have to re-initiate the route discovery process again. The flowchart in Figure 5 gives pictorial description of the various phases in the protocol.

3.1 Performance Evaluation for the RTDSR protocol

The RTDSR protocol was benchmarked with the existing DSR. The performance metrics include: Network Throughput, Average End to End Delay, Routing Overhead and Response Time.

3.1.1 Network Throughput

In MANET, network throughput is the average rate of successful message delivery over 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 packets delivered to the destination to those generated by the source in bits per second (bps), kilobits per second (Kbps) or Megabits per second (Mbps). A high network throughput is desirable for any protocol. One factor that affect throughput in MANET is mobility. The higher the mobilty, the lower the throughput. This is because a higher mobility leads to frequent topology changes which in turn affects data being sent to different destinations. Mathematically, throughput T is expressed using equation 1 as defined in [20],

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

Where: T is the network throughput, C is the total number of connections, f is the unique flow identifier, R_f is the count of packets received, N_f is the count of packets transmitted

3.1.2 Average 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 route discovery latency, queuing at the interface, queue propagation and transfer times. Different applications have different levels of tolerance for delays. While an FTP application can tolerate delay up to a certain threshold, voice and video applications require low delays to avoid jitters. End-to-end delay therefore measures the effective reliability of a routing protocol. A strong factor here is the 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 by [20] 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 packets, *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 the 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 a maximum tolerable delay, after which the data will be useless. Therefore, it is important to provide low delay for real-time flows.

3.1.3 Routing Overhead

Normalized routing overhead is the ratio of routing transmission to the data transmitted during simulation. The routing transmissions are route discovery messages, route reply confirmatory messages and error reply messages. Factors contributing to high overhead includes: size of network, which leads to multiple hops from source to destination. Also the mobility rate, where more links are made and broken arbitrarily when mobility increases. The lower the routing overhead is, the more efficient a protocol will be.

3.1.4 Response Time

For this work we define response time as a measure of the period of time between entry of a request by a remote or local home user and completion of processing for this request. To prevent home users from becoming irritated due to a long download time and intentionally terminating the delivery of an application page, the page transmission time must be within a limited time threshold.

The time it takes for an application page to be completely downloaded on a client's browser can be roughly described using equation 3 as: Total response time R,

$$R = Tc + \sum_{i=1}^{n} Tn_i + Ts \qquad (3)$$

Where: Tc is the client time and is the time spent on the client side. It is the time between start of the transaction, driven by a keyboard or mouse, and the first network outbound event, plus the time from the last network update until the transaction is complete. Tn is the network time. It is the time spent by an application to send the data across the intermediate network. $i = 1 \ldots \ldots \ldots \ldots n$ is the number of intermediate nodes between the client and the server, Ts is the time spent on the server side of the application (for example, the time for a server to query a database) The server has unlimited capacity and unlimited client population. In some cases, the server time can be affected by the network. When packets arrived at the server, the response of the server is determined by the number of client accessing the server at that particular time. The uncertainty of the server time was therefore modeled using the M/M/1 queue system.

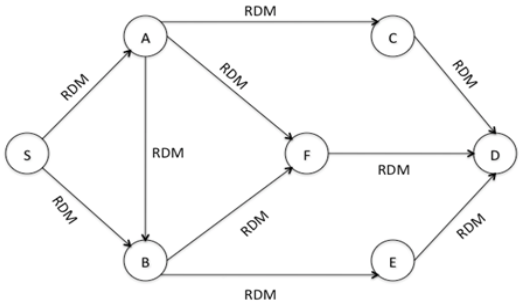

Figure 1: Broadcasting Route Discovery Message

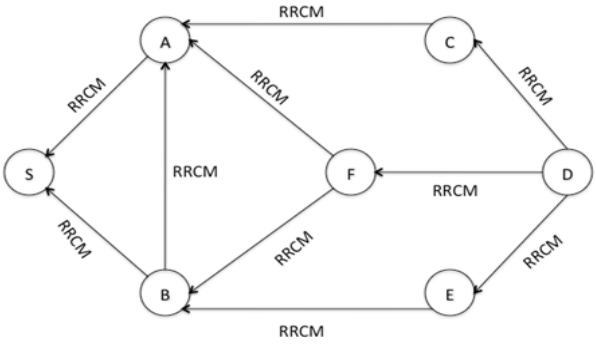

Figure 2: Reply to each Route Discovery Message

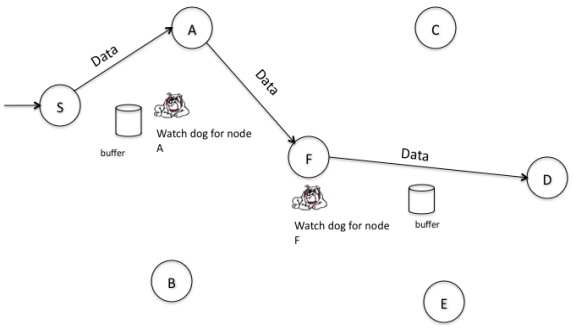

Figure 3: Packet Monitoring through Highly Reputed Path

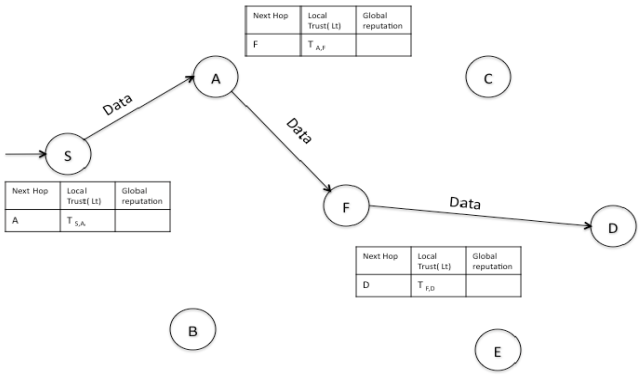

Figure 4: Chosen the Highly Reputed Next Hop Node

Where M/M/1 is exponential inter-arrival time λ, exponential service time μ and single server respectively.

The utilization factor or traffic intensity C_k is defined as:

$$C_k = \left(\frac{\lambda}{\mu}\right)^k = \rho^k \quad \ldots\ldots \qquad (4)$$

Considering the steady state probability of the server π at state k which is π_k

$$\pi_k = C_k \pi_o \qquad (5)$$

Where:

$$\pi_o = \frac{1}{\sum_{k=0}^{\infty} C_k} \qquad (6)$$

Also,

$$\sum_{k=0}^{\infty} C_k = \frac{1}{1-\rho} \qquad \text{provide } \rho < 1 \qquad (7)$$

Thus,

$$\pi_o = 1 - \rho \quad \text{and} \quad \pi_k = \rho^k(1-\rho) \qquad (8)$$

$$\pi_k = \rho^k(1-\rho) \qquad 9)$$

The expected number of client requests in the server L is defines as:

$$L = \frac{\lambda}{\mu - \lambda} \qquad \text{for} \quad \lambda < \mu \qquad (10)$$

The expected number of client requests in the queue is

$$L_q = L - (1 - \pi_0) \qquad (11)$$

Substituting for the value of L and π_0 we have

$$L_q = \frac{\lambda^2}{\mu(\mu - \lambda)} \qquad (12)$$

The expected number of client requests serviced by the server is

$$L_s = L - L_q \qquad (13)$$

The efficiency of the server is

$$E = \frac{L_s}{S} \qquad (14)$$

where S is the number of server

From Little's law we find the waiting time of the client requests.

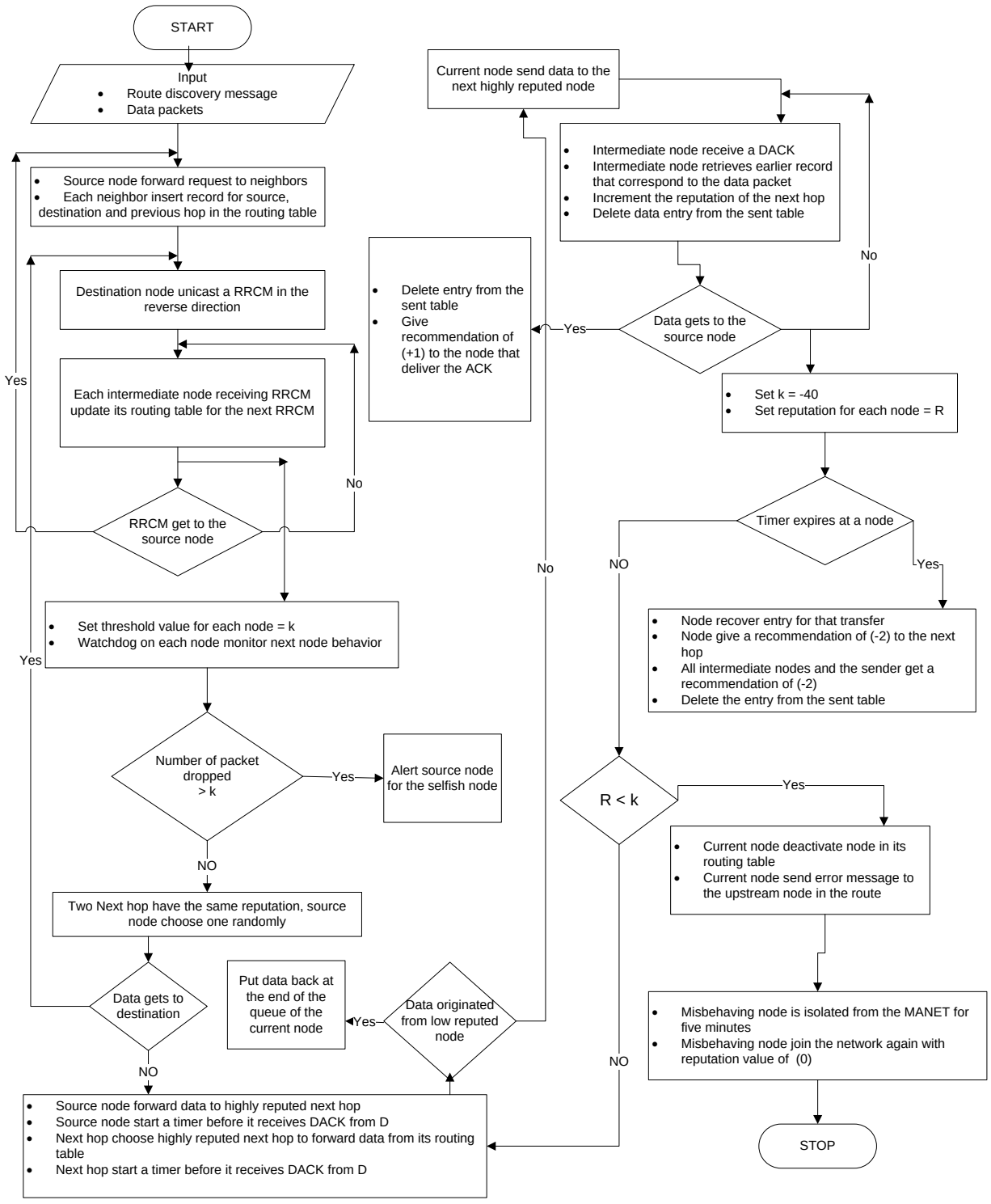

Figure 2: Flowchart for the Proposed RTDSR Protocol

The expected waiting time of client request in the server is

$$W = \frac{\lambda}{\mu - \lambda} \tag{15}$$

The expected waiting time of client request in the queue is

$$W_q = \frac{\lambda}{\mu(\mu - \lambda)} \tag{16}$$

4. DESCRIPTION OF SIMULATION ENVIRONMENT FOR THE CHANNEL ATTACKS PREVENTION MODEL

Simulation was setup for the RTDSR protocol in OPNET 14.5 environment and was benchmark with the existing DSR protocol [3] and [16]. Each node for the RTDSR protocol was configured to have their trust table and watchdog for handling malicious and selfish behaviour respectively. While the existing protocol has a trust

matrix table server and all the connecting nodes communicate with the server for information.

DSR protocol was implemented using office network configuration covering an area of 1.2Km x 1.2Km, with one Fixed WLAN server. We assume that, the number of nodes on the network are 30, 40, 50 and 60. On the WLAN server advanced node model interface, a process called trust matrix table was created as shown in Figure 6. The process was configured to store all the trust values of the connecting nodes. The mobile nodes and the server were spread randomly within the geographical area. Each network design implementation represents a scenario. Scenario one with 30 nodes receives 10 IP unicast traffic while the other scenarios receive 20 IP unicast traffic. The ad hoc routing protocol was set to DSR and TCP traffic was used to study the effects of the protocol. In the profile configuration, FTP application was deployed for our study. All other setting was left at default. The nodes were WLAN mobile clients with a data rate set at 11 Mbps operating with a default power of 0.005 watts. The WLAN server also has a data rate of 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 behaviour . The nodes move at a constant speed of 10 m/s. When the node reaches its destination, it pauses for 300 seconds and then chooses a new random destination. The scenario was simulated for 3600s.

The implementation of RTDSR protocol was carried out by modifying the DSR protocol configuration. The fixed WLAN server was modified to FTP server to serve as destination node for the FTP application. On each WLAN workstation advance node model interface, we created two processes as shown in Figure 7: the trust table process and monitoring watchdog process. The trust table process was configured to store the trust reputation value of connecting nodes. Also the monitoring watchdog process was configured to monitor the next hop on the network against selfish behaviour. Other implementation parameters for DSR protocol were also applicable to the proposed RTDSR protocol. Figure 8 shows the network design environment for (30, 40, 50 and 60) nodes .

5. SIMULATION RESULT AND DISCUSSION

The simulation result for the proposed RTDSR protocol was presented using the following performance metrics: network throughput, delay, routing Overhead and download response time. The RTDSR was benchmarked with the existing DSR protocol.

5.1 Network Throughput

The result in Table 1 indicates a decrease in the performance of the RTDSR protocol except at 50 nodes where 19.620% increase in efficiency was realizes. The DSR protocol has been proven by [16] to have very efficient throughput but the RTDSR protocol was able to maintain slight difference of (12.177%, 13.332% and 26.436% for 30, 40 and 60 nodes respectively) in efficiency. This shows that the data transfer rate of DSR is better than the proposed RTDSR but in some occasions RTDSR can be better.

5.2 Delay

This parameter considered both media access delay and end to end delay. The media access delay was considered because the communication channel will be used for online applications, multimedia and real time traffic. The RTDSR protocol has improved media access delay as shown in Figure 10 for 30 nodes.

The end to end delay recorded increase in performance for RTDSR protocol as shown in Figure 11 for 30 nodes, except for 40 nodes where there was 2.799% decrease in performance. This may be due to changes in network topology as shown in Table 2.

5.3 Routing Overhead

Figure 12 and Table 3 revealed that, the RTDSR protocol had improved performance in routing overhead compared to DSR protocol. Although 50 nodes have 19.866% decrease in performance, this may be because of the wireless nature of the network. The result indicated that the RTDSR protocol sent lighter traffic load such as route request messages, route reply messages and error reply messages.

5.4 Response Time

The download response time as shown in Figure 13 and Table 4 recorded inconsistent improvements for 30, 40, 50 and 60 nodes. The time it takes for the application page to be completely downloaded on the mobile device browser was below 0.2 seconds. Therefore, the RTDSR protocol is efficient to handle download of online applications such as FTP applications, voice and video applications.

6. CONCLUSION

AmI home network designed using mobile devices and MANET will be confronted with serious security challenges because of lack of centralized authority, absence of infrastructure and dynamic network topology. To secure the AmI home communication channel against attacks, a RTDSR protocol was

proposed in this research. The protocol adopted the observation based cooperation enforcement in ad hoc networks (oceans) and collaborative reputation mechanism built on Dynamic Source Routing (DSR) protocol.

In the proposed RTDSR protocol, each mobile ad hoc network node has a trust computation table and a monitoring watchdog to ensure that the next node forward their packet properly. The RTDSR protocol was simulated using OPNET 14.5 modeler and was compared with DSR protocol considering network throughput, delay, routing overhead and response time as performance metrics. Simulation result revealed a better performance of RTDSR protocol over existing DSR protocol. This research work will protect the life in the AmI home against network disruptions that may be caused by malicious and selfish nodes. This research work cannot prevent spoofing attacks, where node will retain a copy of the packet to be forwarded and use it later for malicious purposes. Future work also include subjecting the RTDSR protocol to some attack scenario such as black hole attack.

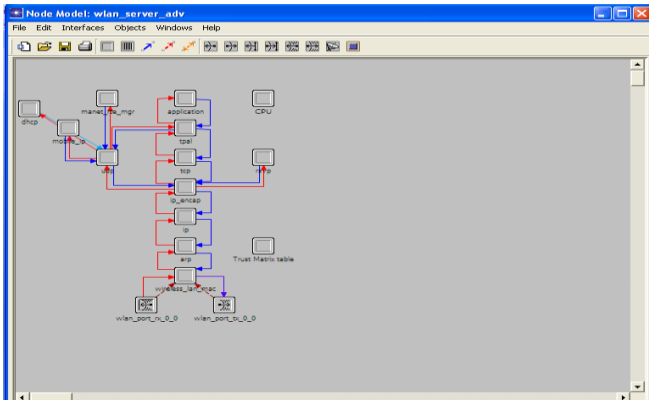

Figure 6: Server Node Model for Trust Matrix Table Process

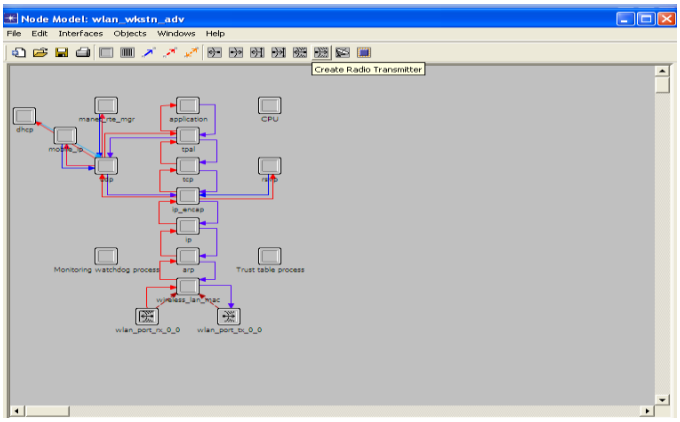

Figure 7: Mobile Ad hoc Node Model for Trust Table and Watchdog Processes

Table 1: Result for Network Throughput (bits/sec) with varying number of nodes

No of Nodes	Average Value for DSR Protocol	Average Value for RTDSR Protocol	Difference in Efficiency (%)	Performance Status
30	63,842	56,912	12.177	Decrease
40	95,505	84,270	13.332	Decrease
50	97,834	121,714	19.620	Increase
60	139,588	110,402	26.436	Decrease

Table 2: Result for End to End Delay (sec) with varying number of nodes

No of Nodes	Average Value for DSR Protocol	Average Value for RTDSR Protocol	Difference in Efficiency (%)	Performance Status
30	0.0031710	0.0028124	12.751	Increase
40	0.0032125	0.0033050	2.799	Decrease
50	0.003827	0.003682	3.938	Increase
60	0.0039243	0.003710	4.776	Increase

Table 3: Result for Routing Overhead (bits/sec) with varying number of nodes

No of Nodes	Average Value for DSR Protocol	Average Value for RTDSR Protocol	Difference in Efficiency (%)	Performance Status
30	62,418	56,080	11.301	Increase
40	93,991	82,764	13.565	Increase
50	95,575	119,269	19.866	Decrease
60	136,181	108,092	24.986	Increase

Table 4: Result for response Time (sec) with varying number of nodes

No of Nodes	Average Value for DSR Protocol	Average Value for RTDSR Protocol	Difference in Efficiency (%)	Performance Status
30	0.13620	0.12695	7.286	Increase
40	0.13009	0.13556	4.035	Decrease
50	0.14834	0.14548	1.965	Increase
60	0.13511	0.15609	13.441	Decrease

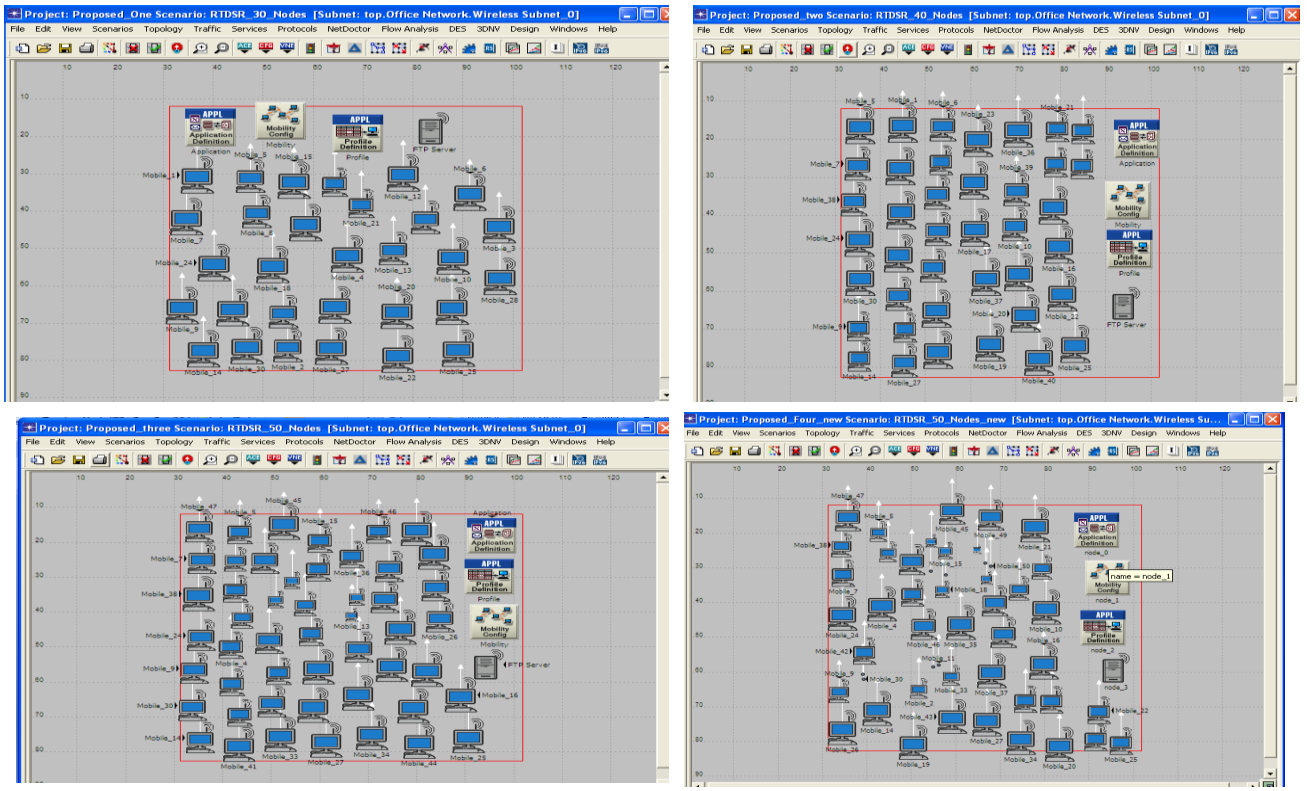

Figure 8: Scenario Network Design Environment for RTDSR Protocol

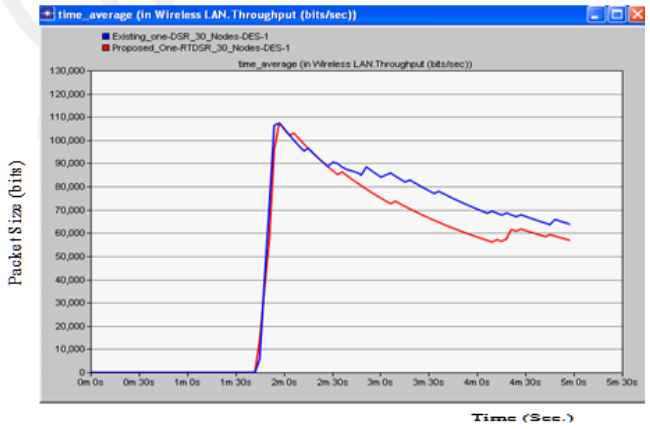

Figure 9: Network Throughput Result for 30 Nodes

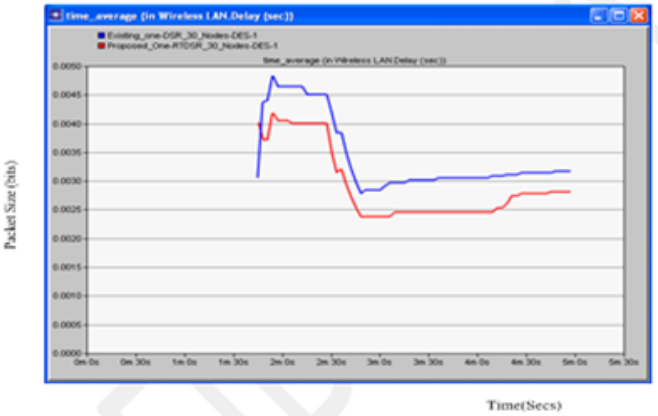

Figure 11: End to End Delay Result for 30 Nodes

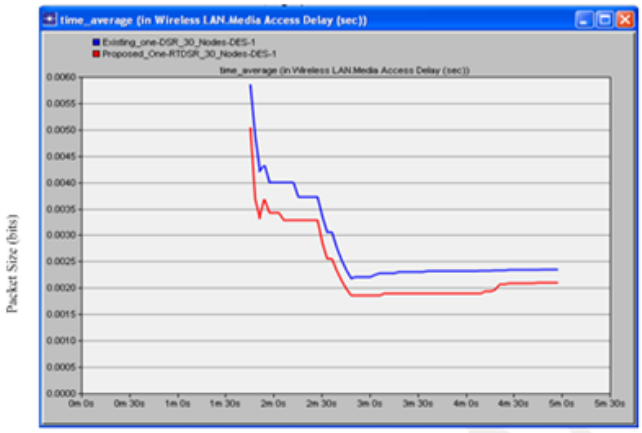

Figure 10: Media Access Delay Result for 30 Nodes

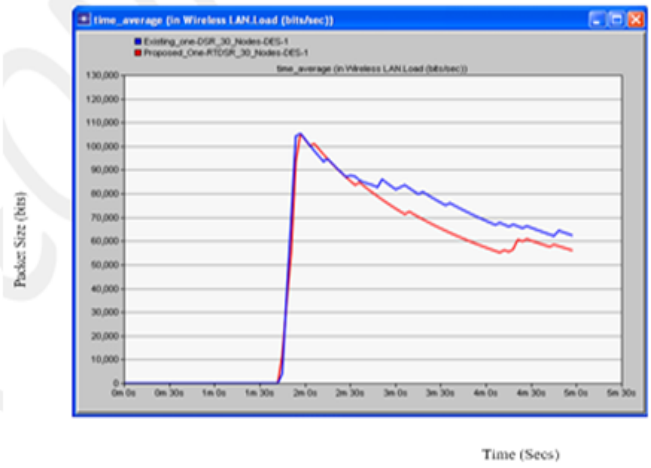

Figure 12: Routing Overhead Result for 30 Nodes

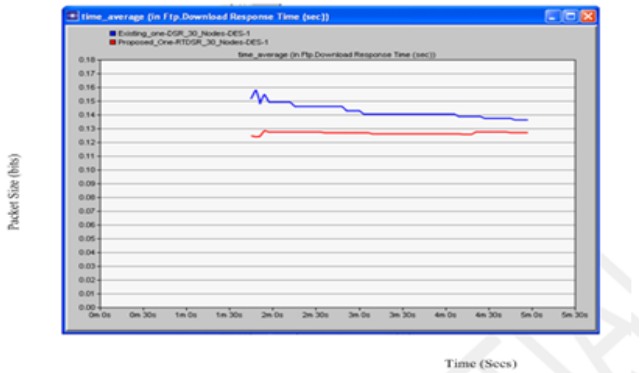

Figure 13: Download Response Time Result for 30 Nodes

REFERENCES

[1] Giacomo, C., Luca, F., Letizia, L. and Franco, Z. Connecting Ambient Intelligent Components via Dedicated Middleware: an Agent Approach. 14th *IEEE international workshops on enabling technologies*: infrastructure for collaborative enterprise INETICE' 05, pp. 39-46, 2005.

[2] Mariano, A. and Beatriz, R. New Technologies for Ambient Intelligence. IOS Press, G. Riva, F. Vatalaro, F. Davide and M. Alcaniz, pp. 17-25, 2005.

[3] Zheng, Y.; Peng, Z. and Teemupekka, V. Trust Evaluation Based Security Solution in Ad hoc Networks. *The Seventh Nordic Workshop on Secure IT System Nordsec* 2003, Gjovik, Norway. 8(2), pp. 236-243, 2003.

[4] Gagandeep S.H, Sunil K. G. and Rajeev B. Adaptive Approach to Find a Stable Path Between Nodes in MANET. *International journal of current engineering and technology* 4(4) pp 898-901, 2014.

[5] Selvakanmani S. and Sumathi M., An opportunistics Routing protocol for Mobile Cognitive Radio Ad hoc Networks. *International Journal of engineering and Technology* 6(2), pp 692-700, 2014.

[6] Mecnatchi I. and Palanivel K. An Enhanced Cross Layer Intrusion Detection and Adaptive Response Mechanism for MANETs. *International journal advanced research in computer engineering and technology* 4(3), pp 998-1004, 2015.

[7] Bakhouya M., Gaber J., and Loreuz P., Energy evaluation of AID Protocol in Mobile Ad hoc Networks. *Elsevier Journal of Network and Computer Application,* Vol 58, pp287-293, 2015.

[8] Mahmoud Sami, Noordin Nor Kamariah, Fazirulhysiam Hashim, Shamala Subramaniam, Ayyoub Akbari-Moghanjoughi, An Energy-Aware Cross-layer Cooperative MAC Protocol for Wireless Ad hoc Networks. *Elsevier Journal of network and Computer Applications,* Vol. 58, pp 227-240, 2015.

[9] Sukumran, Sangheetaa; Jaganathan, Venkatesh and Korath, Arun Reputation Based Dynamic Source Routing Protocol for MANET. *International Journal of Computer Applications*, 47(1), pp. 42-46. 2012,

[10] Lyno Henrique Ferraz, Pedro Velloso, Otto Carlos Duarte An accurate and precise malicious node exclusion mechanism for ad hoc networks. *Elsevier Journal of Ad Hoc Networks* Vol. 19, 142-155. 2014,

[11] Jun-Won Ho, Matthew Wright , Sajal K. Das Distributed detection of mobile Malicious node attacks in wireless sensor networks. *Elsevier Journal of Ad Hoc Networks* 10(3) 512-523. 2012,

[12] Hongjun D.; Zhiping J. and Zhiwei Q. Trust Evaluation and Dynamic Routing Decision Based on Fuzzy Theory for MANETs. *Journal of software* 4(10) pp 1091- 1099. 2009.

[13] Arathy K.; and Sminesh C. "A Novel Approach for Detection of Single and Collaborative Black Hole Attacks in MANET". ELSEVIER *Journal of Global Colloquium in Recent Advancement and Effectual Researches in Engineering, Science and Technology. Procedia Technology* Vol.25. Pp 264 – 271, 2016.

[14] Rahul J.; Rishabh G.; Rashmi.; and Sandhya K. "Detection and prevention of wormhole attack in ad-hoc network using AODV protocol". *International Journal of Computer Science and Mobile Computing*. Vol.6. Issue 4 Pp 241 – 248, 2017.

[15] Burhan U.; Rashidah F.; Asifa M.; Nurul F.; and Sajad A.. "Secured Trust-Based Communication Method in Vulnerable Mobile Ad-hoc Network" *SPRINGER Journal of International Conference on Robotic, Vision, Signal Processing and Power Applications.* Pp 149 – 160, 2017.

[16] Khaleel, U.; Khan, R. and Reddy, V. Performance Comparison of on-Demand and Table Driven Ad Hoc Routing Protocol using NCTUns. *Proceedings of 10th International Conference on Computer Modeling and Simulation* UK, 7(2), pp. 336-341. 2008.

[17] Yaser Khamayseh, Ruba Al-salah, Muneer Bani Yassein, Malicious Nodes Detection in MANETs: Behavioral Analysis Approach. *Journal of networks*, 7(1), pp 116-125, 2012.

[18] Kumar Jaspal, Kulkami M., and Daya Gupta, Effect of Black Hole Attack on MANET Routing Protocols. *International Journal of Computer Network and Information Security* Vol. 5, pp 64-72, 2013.

[19] Ingrid, V.; Alireza, H.; David, H. and Bo-cheng, L. Security for Ambient Intelligent System, Springer-Verlag, 199-221, www.broks.google.com 2005.

[20] Gupta, A. K.; Sadawarti, H. and Verma, A. K.. Performance Analysis of AODV, DSR and TORA Routing protocols. *International Journal of Engineering and Technology*, 2(2), pp 226-231. 2010