Int. J. Communications, Network and System Sciences, 2015, 8, 19-28
Published Online March 2015 in SciRes. http://www.scirp.org/journal/ijcns
http://dx.doi.org/10.4236/ijcns.2015.83003

Lightweight Robust Forwarding Scheme for Multi-Hop Wireless Networks

Arif Sari

Department of Management Information Systems, European University of Lefke, Lefke, Cyprus
Email: asari@eul.edu.tr

Received 21 October 2014; accepted 27 February 2015; published 5 March 2015

Abstract

The Gossip-Based Relay Protocol (GRP) is developed based on *Ad Hoc* on Demand Distance Vector Protocol (AODV) and proposed to increase the efficiency of package routing functionality in *ad hoc* networks through specific flooding scheme. This lightweight protocol reduced the collisions on the network through specific mechanisms. Request to Send/Clear to Send (RTS/CTS) mechanism is widely used in *ad hoc* environment with Temporarily Ordered Routing Algorithm (TORA) in order to eliminate collisions and allow access to the shared medium through proposed authentication methods. Since GRP contains specific mechanism of directed acyclic Graph (DAG) mechanism to mitigate overhead problem, RTS/CTS modified TORA might result in similar performance metrics. In this paper, TORA protocol has a modification of new RTS/CTS mechanism and has been simulated in order to be compared with proposed lightweight robust forwarding GRP scheme in terms of specific performance metrics such as network throughput, end-to-end delay and message flooding rate over the network through OPNET simulation package in order to expose the optimal solution to increase overall network throughput in *ad hoc* environment.

Keywords

GRP, TORA, RTS/CTS Mechanism, OPNET Simulation, Throughput, Robust Forwarding Scheme

1. Introduction

Dynamically calculated routing tables and exchange of dynamic routing information among mobile nodes are inevitable for existence of multi-hop networks due to their nature characteristics. The *ad hoc* environment provides an opportunity to deploy a simple network without requesting any pre-identified network infrastructure. The lightweight wireless devices which participate in these networks relay the user information on the network and do not generate any dynamic routing information to communicate with other devices. Authentication is

How to cite this paper: Sari, A. (2015) Lightweight Robust Forwarding Scheme for Multi-Hop Wireless Networks. *Int. J. Communications, Network and System Sciences*, **8**, 19-28. http://dx.doi.org/10.4236/ijcns.2015.83003

prominent for an *ad hoc* environment since dynamic routing information is crucial for secure data transfer among participating nodes. On the other hand, due to mobility and dynamic nature of multi-hop wireless networks, participating nodes may not reliable to share static routing information and generation of dynamic routing information becomes a certain issue.

Researchers have discussed Gossip Relay protocols in the literature however there is no detailed research available to evaluate security aspects of GRP since it is designed to enhance performance. The implementation of the GRP relays on the probabilistic method to determine the priority of the message to broadcast by assigning a rate of probability. RTS/CTS mechanism with TORA protocol is used to provide an authentication between sender and receiver so it also creates dynamic routing information with different proposed methods similar to GRP where it aims to decrease the broadcast messages on the network without requesting any explicit route setup. The dynamic nature of wireless networks requires lightweight security mechanisms in order to tackle limitations of basic network infrastructure and to enhance effectiveness and efficiency of the network. Aim of this research paper is to expose the impact of different lightweight routing mechanisms on multi-hop wireless networks in terms of different network performance metrics. In the organization of this research paper, the first section discusses current researchers conducted on the basis of GRP protocol on the basis of parent child and siblings relationship theory. The next section covers formulation of simulation scenario for proposed mechanisms in OPNET simulation environment and findings section discusses the simulation outcomes to expose the optimal algorithm to use in multi-hop wireless networks. In the next section, all these lightweight robust mechanisms are shown and explained in details and each of the proposed method is simulated in OPNET environment to compare and expose the optimal algorithm or method to use in multi-hop wireless networks.

2. Literature Review

GRP is proposed by the researchers in the literature with an idea of reducing broadcasted messages by a probabilistic method and determine whether a participating node will broadcast the received message or not [1]. The implementation of GRP is designed based on AODV protocol by the researchers which require route calculation and choose the best route to use and forward the messages. Other researchers have proposed another routing efficient algorithm by clustering the participating nodes into subset of neighbors which is efficient and nodes used to forward broadcasted message to the corresponding neighbors rather than sending to entire network [2] [3]. The GRP protocol relay on a deterministic approach with probabilistic function in order to reduce message flooding on the network to prevent overhead problem. Based on the GRP protocol, the MAC protocol is modified for CSMA/CA (Collision Avoidance) feature to implement such mechanism on the network. The proposed GRP protocol is used to conduct Parent-Sibling-Child (PSC) relationship for direct traffic flows which clearly shown in the literature [4]. The PSC relationship leads participating nodes to be clustered into such hierarchy to forward broadcasted received message only to it's corresponding relative, e.g. child or sibling. **Figures 1-3** illustrate the relationship between parent-child-sibling techniques below. Each of the relationship illustrated on the figures have a specific probability formulas which were shown on the formulas below. The P_n represents the broadcast probability where n is received packages. The increased probability for packets received from parent is shown in Equation (1) below [4];

$$P_n = P_{n-1} + \left(1 - P_{n-1}\right) * 2^{-3} \tag{1}$$

where decreased probability for packets received from sibling shown in the Equation (2) below [4],

$$P_n = P_{n-1} * \left(1 - \left(2^{-4}\right)\right) \tag{2}$$

where n is the nth new message package and $n - 1$ is the $n - 1$th message package.
The basic purpose of this method is to purpose package broadcast mechanism from the parent node rather than from the siblings. This mechanism creates kind of virtual clusters among nodes. **Figure 1** presents parent diagram for direct traffic flows in proposed GRP parent-sibling-child mechanism.

The parent node A is responsible of spreading packages to its siblings which prevents B and C nodes to broadcast redundant packages to A and mitigate overhead problem.

Figure 2 illustrates the sibling relationship between nodes.

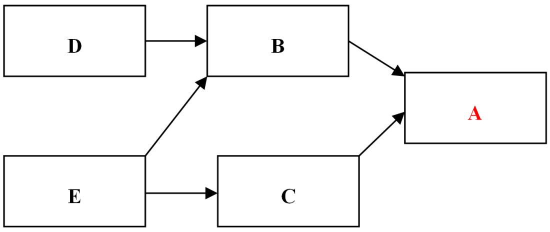


Figure 1. Parent diagram.

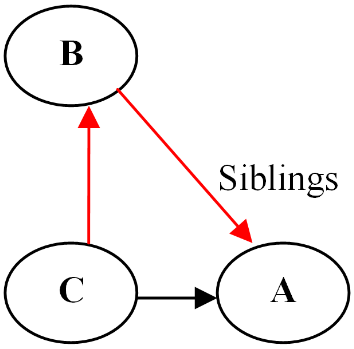


Figure 2. Sibling diagram.

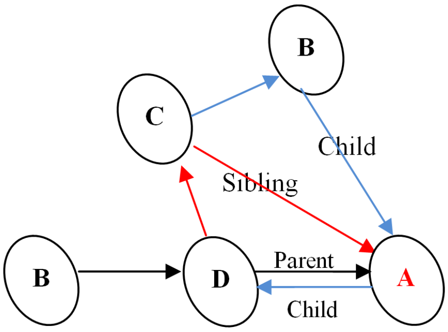


Figure 3. Child diagram.

As it is presented in the Figure 2, B becomes sibling of A and transfers particular segment to A while corresponding segment contains a message stating that the parent for B is C. This implementation decreases the probability of broadcast of messages from siblings.

Figure 3 above illustrates the child diagram mechanism. The figure presents 2 different cases where A receives a messages from D, that approves D is the parent of A. Meanwhile if A receives a package from B, which the parent of B is C, which is the sibling of A, hence to A, B takes the role of a child.

Request to Send (RTS), Clear to Send (CTS) and Fragmentation Thresholds impact on AODV protocol are well known by the simulation experiments conducted in this study and RTS implementation is done in order to increase the performance of the network. Figure 4 illustrates the basic working mechanism of RTS/CTS. In other cases, RTS/CTS is the optional mechanism used by the 802.11 wireless networking protocols to reduce frame collisions introduced by the hidden node problems [5]. The impact of RTS/CTS mechanism is clearly stated by the researchers and exposed through simulation experiment in the literature. However, in order to analyze the difference between the GRP and RTS/CTS under TORA protocol and expose the most optimal way solution for multi-hop wireless networks, it is necessary to conduct a simulation experiment. Variety of studies conducted in the literature to solve security dilemma of wireless networks and researchers have proposed variety of solutions for 802.11 mobile wireless environment security challenges [6]-[8]. Researchers have conducted simulation experiment in order to expose findings of their study. The next section gives brief description about

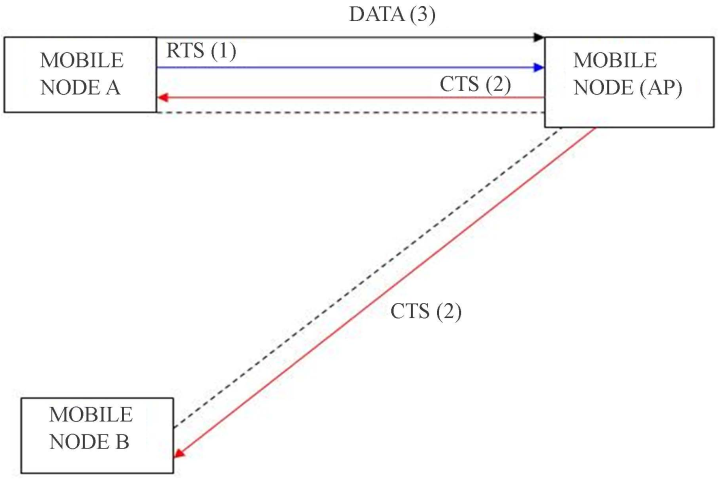


Figure 4. RTS/CTS mechanism.

simulation experiment designed in this study.

2.1. TORA and RTS/CTS Mechanism

TORA is a transport layer protocol for better performance to limit control message propagation in the highly dynamic mobile computing. The basic role of TORA is to create a route from a source to destination, maintain the corresponding route within specific time intervals in order to adopt changes of the dynamic nature of mobile routing. The working mechanism of this protocol belongs to a class of algorithms called link reversal algorithms. The TORA protocol has an ability to adopt route changes in Mobile Wireless Networks by creating destination disoriented graphs. The partial or full reversal algorithms are used to create and maintain in a case of any changes in the network.

The directed acyclic graph (DAG) is created from the source to destination which is represented as G(V,E) where V represents nodes and E represents edges in a graph. This DAG contains multiple routes for routing table to destinations. Main idea of using DAG is to build a routing information and links between source nodes to destination and recomputed the DAG through link reversal algorithms in a case of any failure on links.

Three basic message type is used by TORA which are QRY, UPD and CLR where;

QRY is used to create a new route;

UPD is used to maintain existing routes;

CLR is used for erasing existing routes.

TORA protocol has an advantage of using DAG mechanism in a case of demand to create multiple paths. The on-demand protocols like DSR can be used to perform similar tasks like TORA, however due to performance issues of delivering data frames on network; TORA protocol is preferred in this research.

The Request to Send/Clear to Send (RTS/CTS) is an optional mechanism applied in wireless networks in order to avoid frame/Segment collision. This method is also implemented to realize virtual carrier sensing in the Carrier Sense Multiple Access with collision avoidance (CSMA/CA). It is clearly stated above that, TORA protocol using specific messages to create, maintain or erase new routes on the network within specific time intervals. However, corresponding route maintenance messages may not reach to its destination due to variety of problems (e.g. internal or external attacks, misbehaving node, hidden node etc.) and it may simply cause negative impact on overall performance of the network. The RTS/CTS new frame format is shown on the Table 1.

2.2. GRP Algorithm

The Algorithm (1) represents the pseudo-code of the Gossip Relay Protocol used in this research. The relationship contains 4 different structural conditions to differentiate between PSC relationships. In the proposed algorithm, GRP(t) represents overall algorithm where (t) is a package and passing corresponding information to the MAC layer.

Algorithm (1) : GRP(t)

```
START with GRP (t)
IF (segmenttarrives first time from node x)
THEN
    Update status of node a as a parent node
    Increase broadcast probability of segments from node a
    Send t to MAC
ELSE
t is not arrived as a new segment from node a
        IF (t from different grandparents and different parents ||
        t from same grandparents and different parents)
    THEN
                Update status of node x as a parent node
    Increase broadcast probability of segments from node a
        Send t to MAC
      ELSE
                IF(t from node x whose the grand parent is "me")
                THEN
                        Update node x as my child
                        Set the broadcast probability p = 0.0
                        Stop and exit.
                ELSE
                        IF(t from node a whose grandparent is my parent)
                        THEN
                              Update status of node a as sibling
                              Decrease its probability p
                              IF (GRP is TRUE)
                              THEN
Send t to MAC
                              ELSE Exit
                 Exit
```

Table 1. RTS/CTS new frame format.

RTS FRAME
Frame Control
Duration
Receiver Address
Transmitter Address
Frame Check Sequence
ACK FRAME
Frame Control
Duration
Receiver Address
Frame Check Sequence
CTS FRAME
Frame Control
Duration
Receiver Address
Frame Check Sequence

3. Simulation Experiment

The tool used for the simulation study is OPNET 14.0 modeler. OPNET is a network and application based software used for network management and analysis where it provides variety of simulation samples with Graphical User Interface (GUI) along with the considerable amount of documentation and study cases for wired as well as wireless networks [9]. In this research, 2 different scenarios are used and illustrated through OPNET simulation package. In the first scenario, GRP protocol is simulated and in second scenario RTS/CTS mechanism is simulated. The attributes and parameters set for the creation of the simulation environment for scenario 1 in OPNET shown on the **Table 2** in details below.

The performance metrics set for this experiment are shown on **Table 2**. According to the values of **Table 2**;

Throughput; is the rate of successful messages delivered from source point to destination node over a communication channel through wired or wireless media.

End-to-end delay; is the time taken for the segment/datagram to be transmitted across a network from source to destination and represented as;

dend-end = N [dtrans + dprop + dproc]

where;

dend-end = end-to-end delay

dtrans = transmission delay

dprop = propagation delay

dproc = processing delay

dqueue = Queuing delay

N = number of links (Number of routers + 1).

Network Load; is amount of package (segment/datagram) traffic being carried by the network.

The attributes and parameters set for the creation of the simulation environment for scenario 2 in OPNET simulation package shown on the **Table 3** in details below.

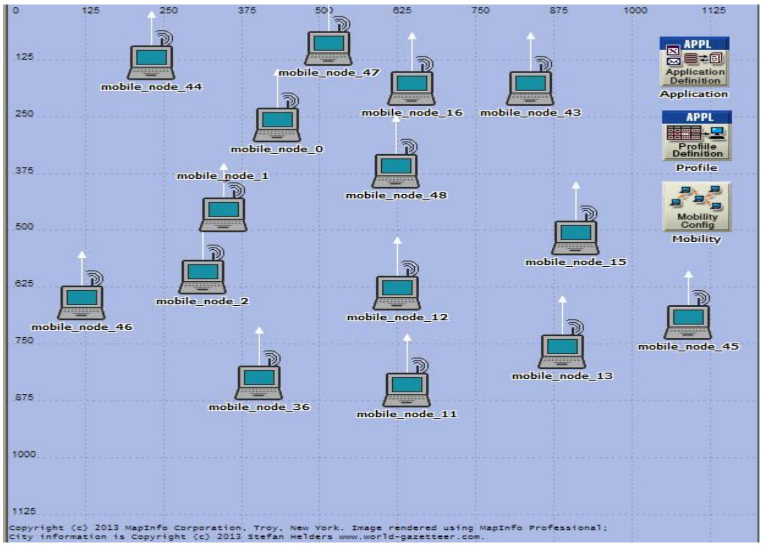
Figure 5 illustrates the simulation setup of a single scenario which can be considered as an global scenario since there is no difference between two scenarios in terms of number of participants on the network where comprising of 15 active mobile nodes move around at a specific constant speed of 10 meters per seconds. In this research, 2 scenarios have been developed by setting the specific mobility value of 10 m/s. while the complete simulation duration set to be conducted for 300 seconds. The area for simulation arranged as campus area of

Table 2. Global parameters for GRP network—scenario 1.

Parameter	Attribute
Protocol	GRP (AODV based)
Simulation Duration	120 (seconds) with 300 seed
Simulation Area	1000 × 1000 meters
Mobility	Random Waypoint
Performance Metrics	Throughput, Delay, Load
No of Nodes	15

Table 3. Global parameters for TORA with RTS/CTS network—scenario 2.

Parameter	Attribute
Protocol	TORA
Simulation Duration	120 (seconds) with 300 seed
Simulation Area	1000 × 1000 meters
Mobility	Random Waypoint
Performance Metrics	Throughput, Delay, Load
No of Nodes	15



Copyright (c) 2013 MapInfo Corporation, Troy, New York. Image rendered using MapInfo Professional;
City information is Copyright (c) 2013 Stefan Helders www.world-gazetteer.com.

Figure 5. Simulation environment for 15 nodes.

1000 × 1000 meters. The exponential value of 0.3 is set for packet inter-arrival time and generated packet size is set as exponentially 2000 bits. Mobile node data rate is set to 11Mbps with a default transmitting power of 0.005 Watts. Mobile nodes move around with random way point mobility with a constant speed of 10 meter/sec while the pause time is set to 100 seconds. This pause time is taken after the corresponding generated data reaches it's' destination only.

The simulation run time is set as 300 seconds which is equal to 60 minutes with the seed value of 300. Simulation Kernel is set to "optimization". Application profile, Profile configuration, and Mobility are configured to work on the network in order to provide data flow over the network.

4. Simulation Results

The OPNET simulation package provides two different types of statistics which are known as Global and Object statistics in order to evaluate the performance metrics or the entire simulation outcomes. The global statistics represents the collection of entire network's data and analysis. The object statistics involves individual nodes statistics. In this simulation experiment, the global discrete event statistics (DES) statistics are taken into consideration for evaluation of performance metrics.

This section focuses on results, its analysis and comparison based on the simulation performed in OPNET modeler 14.0. Based on the parameters set for the simulation scenarios (scenario 1 and scenario 2), the WLAN throughput of both mechanisms are illustrated in **Figure 6**.

As it is clearly shown on the **Figure 6**, there is significant difference between GRP and RTS/CTS mechanisms. Overall throughput of the network in terms of bits/seconds is significantly decreased when an RTS/CTS mechanism is used with TORA protocol.

Figure 7 indicates simulation results of average WLAN Delay. The packet end-to-end delay representing the average time in order to traverse the packet inside the network. This value contains the time frame from the generation of the segment from the sender until the reception of the segment by the receiver and it is expressed in seconds.

Figure 8 shows the average WLAN Delay. Since the RTS/CTS mechanism proposes a handshaking mechanism in order to authentication and aims to eliminate hidden node problem and in contrast to this GRP uses CSMA/CA collision avoidance features, the high rate of WLAN Delay is expected from RTS/CTS scenario.

Finally, **Figure 8** shows the average network load, which is the total traffic received by the whole network from higher layer of MAC that is accepted and queued for the corresponding transmission. It represents the amount of traffic in the overall network. It also indicates the total data traffic in bps received by the overall network from higher MAC layer accepted and queued for transmission.

As it shown in the **Figure 8**, GRP protocol remains faster and contain much network load than TORA

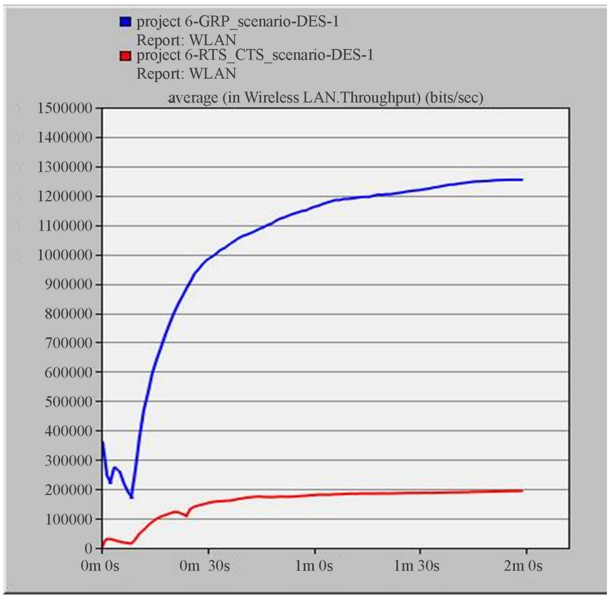


Figure 6. WLAN throughput of GRP and TORA with RTS/CTS mechanisms.

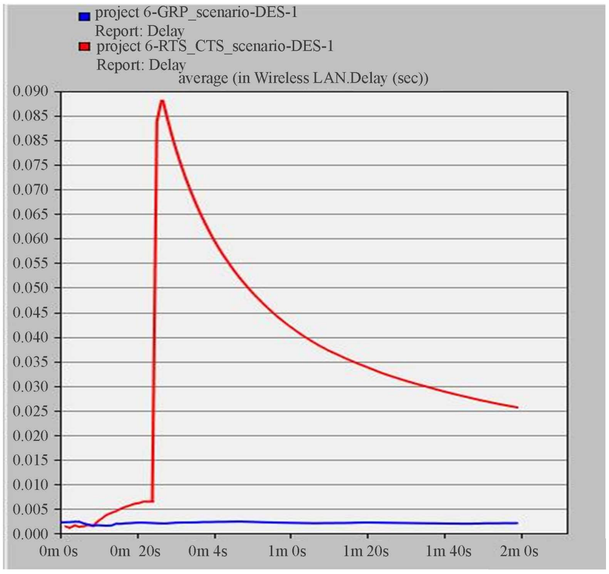


Figure 7. Average WLAN Delay of GRP and TORA with RTS/CTS mechanism.

protocol with RTS/CTS mechanism. The high rate of load represents low rate of data dropped on the network due to collisions or some other reasons. However this may indicate the high rate of overhead problems since there is no differentiation of packages received as broadcasted message.

5. Conclusion

The performance of GRP (with simplified MAC protocol) and TORA protocol (with embedded RTS/CTS mechanism) is simulated and compared. The GRP is found to deliver much better performance than the TORA protocol in terms of Throughput, Delay and Network Load. Since high rate of broadcasted packages is delivering to the base station through participating nodes in contrast to TORA protocol, it can be considered that GRP is successful. However, the Base Stations used in GRP protocol are fixed and it is also stated in previous studies.

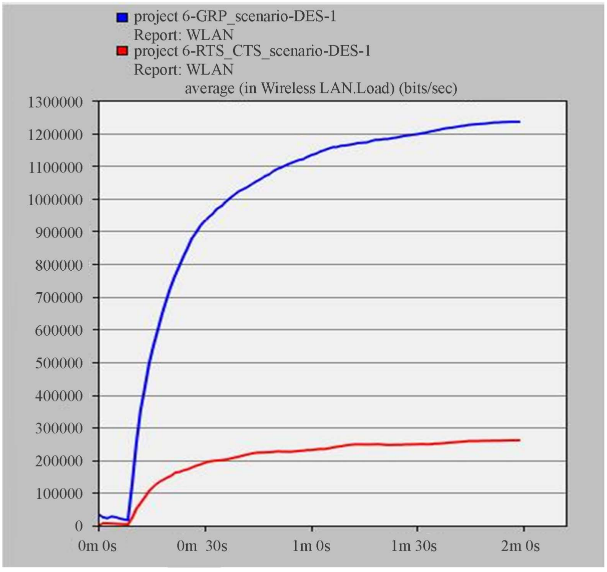


Figure 8. Average network load.

This may lead to exposure for a need of a better probability function to work in more flexible situations where mobility is a serious concern for multi-hop wireless networks. As it is mentioned in the previous section, the overhead problem remains as an unsolved issue since there is a constant data flooding mechanism used in GRP with PSC relationship and no differentiation among packages is specified. Researchers should investigate how to differentiate the forwarding of broadcasted messages to minimize overhead problem for bi-directional data transfers and also in terms of transferred data security.

6. Future Recommendations

The purpose of implementation RTS/CTS mechanism on TORA protocol was eliminating imbalance between GRP and TORA. However, results indicated that the RTS/CTS mechanism has an update and includes ACKs which has a significant contribution to leading an overhead problem. Researchers should focus on specific mechanisms or propose new mechanisms to decrease overall overhead on the network by improving RTS/CTS mechanism for TORA protocol. On the other hand, GRP protocol should be examined in more crowded networks to expose overall network load, data drop rate and network throughput to understand its performance during mobility.

References

[1] Hass, Z., Halpern, J.Y. and Li, L. (2002) Gossip-Based *ad Hoc* Routing. *IEEE/ACM Transactions on Networking* (*ToN*), **14**, 479-491.

[2] Paruchuri, V.K., Durresi, A., Dash, D.S. and Jain, R. (2003) Optimal Flooding Protocol for Routing in *Ad-Hoc* Networks. *IEEE Wireless Communications and Networking Conference*, March 2003, 93-102.

[3] Calinescu, G., Mandoiu, I., Wan, P.-J. and Zelikovsky, A. (2004) Selecting Forwarding Neighbors in Wireless *ad Hoc* Networks. *Mobile Networks and Application*, **9**, 1-23.

[4] Maeung, S., Yang, S.J. and Shenoy, N. (2004) Modelling and Analysis of Gossip Based Relay Networks for Ubiquitous and Extended Access. *OPNETWORK* 2004, Washington DC, 30 August-3 September 2004, 1-5.

[5] Sari, A. and Necat, B. (2012) Impact of RTS Mechanism on TORA and AODV Protocol's Performance in Mobile *ad Hoc* Networks. *International Journal of Science and Advanced Technology* (*IJSAT*), **2**, 188-191.

[6] Sari, A. (2014) Security Approaches in IEEE 802.11 MANET. *International Journal of Communications*, *Network and System Sciences*, **7**, 365-372. http://dx.doi.org/10.4236/ijcns.2014.79038

[7] Sari, A. and Rahnama, B. (2013) Simulation of 802.11 Physical Layer Attacks in MANET. 2013 *Fifth International Conference on Computational Intelligence*, *Communication Systems and Networks* (*CICSyN*), Madrid, 5-7 June 2013, 334-337. http://dx.doi.org/10.1109/CICSYN.2013.79

[8] Sari, A. (2014) Security Issues in RFID Middleware Systems: A Case of Network Layer Attacks: Proposed EPC Implementation for Network Layer Attacks. *Transactions on Networks & Communications*, *Society for Science and Education*, *United Kingdom*, **2**, 1-6. http://dx.doi.org/10.14738/tnc.25.431

[9] OPNET Technologies Inc. Opnet Simulator. www.opnet.com