Journal of Engineering and Applied Sciences 14 (8): 2550-2552, 2019
ISSN: 1816-949X

# Enhance of Security in AODV Protocol using Cross Layer Design

Omar A. Salam Abdulkareem
Research and Development Directory, Ministry of Higher Education and Scientific Research,
Baghdad, Iraq

**Abstract:** Ad-hoc networks are smart protocol that service the technology and is used in many applications such as rescue and strategic operations, due to the suppleness provided by their active structure. However, this suppleness is attended with new security threats. Moreover, many developed security solutions used for wired networks are unsuccessful and unproductive for the highly dynamic and use wide of resources where MANET resources are limited expected. In this study a proposed of Cross Layer Based Defense Enhancement Technique “CBDET” to solve this problem.

**Key words:** WSN, AODV, MTR, MATLAB, PDR, security threats

## INTRODUCTION

**Mobile Ad-hoc Network:** “MANET” stands for “Mobile Ad-hoc Network”. It is an infrastructure less wireless network because of movement of the nodes are randomly resulting in a dynamic topography. (Rajaram and Palaniswami, 2009). In “MANET”, nodes communicates directly with other nodes with a borders of their radio broadcasting range. An intermediate nodes used to communicate as a relay between two or more nodes in order to receive and send data in between from to other nodes if the nodes are not in range then the source nodes uses an intermediate node to communicate with distention node (Li and Joshi, 2008). Ad-hoc is a protocol defined for a network in which a set of wireless nodes communicate straight with one another without using an Access Point “AP” or any infrastructure network. Moreover, nodes are moves free and randomly and they self-organize. By Gopinath *et al.* (2012) a “MANET” applications covers emergency search and rescue processes in data acquisition processes in hostile land and etc., (Rachedi and Benslimane, 2009). Cooperative behavior is the nature of nodes in “MANET” of its neighbor nodes has high security fears. In addition the attack on “ad-hoc” network can come from any direction at any node that is different from the fixed and wired networks with physical protection using firewall gateways or shields.

**Security attacks in MANET:** The features of MANET and other infrastructure less network, the mobility of the nodes, “closure communication medium”, “lack of centralized control” and topology unexpected changes makes it in high security risks.

And the use of wireless communication channels makes “MANETs” susceptible to network attacks (Suresh and Chandra, 2008). In addition “MANET” the security in this networks is completely dissimilar compared to any other network structures such as wired networks and the attacks are occurred from any node on the network coverage or network range. Therefore, each wireless mobile node in the network must secured with a security mechanisms.

**Cross-layer design:** Cross-layer design in “MANETs” networks has a different considerations according to its inherent characteristics of the network including “unexpected change in topology”, “unexpected capacity”, ”required bandwidth”, “energy constraints nodes”. Thus all of these features are extremely challenged and permit to create a new way and methodology named “cross-layer”.

As known that the “cross-layer design” goes beyond the standards network design where each layer on the OSI model of the protocol stack operates separately and has the capability to exchanges information with adjacent layers only through a narrow interface (Babu and Sekharaiah, 2013).

## MATERIALS AND METHODS

**Cross layer based defense enhancement technique:** “CBDET” is a mechanism that is capable of detecting the malicious nodes and to deliver security by steering the “AODV” routing path escaping the malicious node.

**Energy at each node:** Each node calculates its Energy (Er), using energy model.

$$iEnergy = iNode \rightarrow energy - model() \rightarrow energy() \qquad (1)$$

(in aodv.cc) iNode = present node iEnergy = Er, Residual energy of that particular node. Deciding the threshold values energy Consumption of each node in the network coverage is the transmission and the reception of data or controlling packets such as “RREQ”, “RREP”, “RERR”, “HELLO”. So, it a predicted and expected value on each node thus a threshold value can be set.

**Proposed algorithm:**

```
If source node A require to send data to distention node B then
{AODV ( )// to finds a route between A and B
{For (each node donating in communication amongst A and B)
{Calculate energy of each node using energy model to present the energy of each node (Er)
When any node receives a packet
{If (Ethl<Er<Ethu)
{Receive RREQ packet and forward it to next Hop.}
Else {Drop RREQ Packet and It sends another RERR to the last node in hop and the source node “need to call AODV () again”}
}}}}}
```

## RESULTS AND DISCUSSION

NS2 was found is the best environment for this simulation a 27 nodes was created and configured as MANET with AODV and Ad-hoc with characteristics shown in the following Table 1.

Table 1: NS2 simulation parameters

| Parameters | Values |
|---|---|
| Routing protocol | AODV |
| Propagation model | Two ray ground |
| No. of nodes | 27 |
| Environment size | 700*510 |
| Traffic type | TCP |
| MAC | 802-11 |
| Initial Energy | 100 |
| Queue length | 50 |

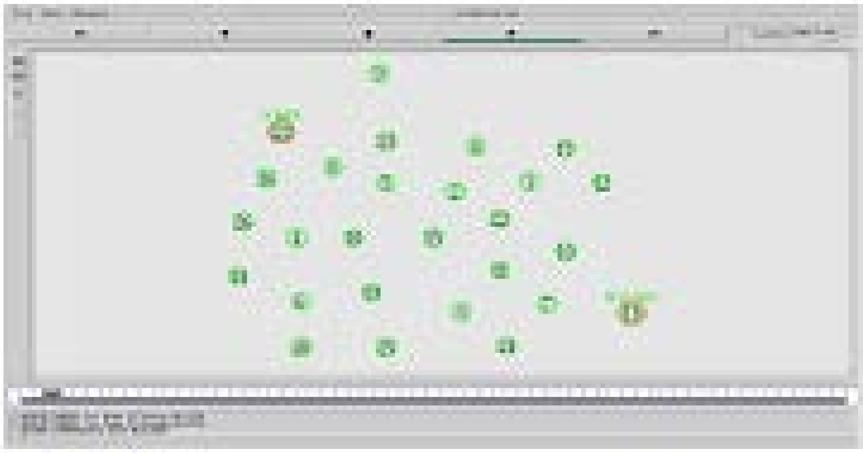
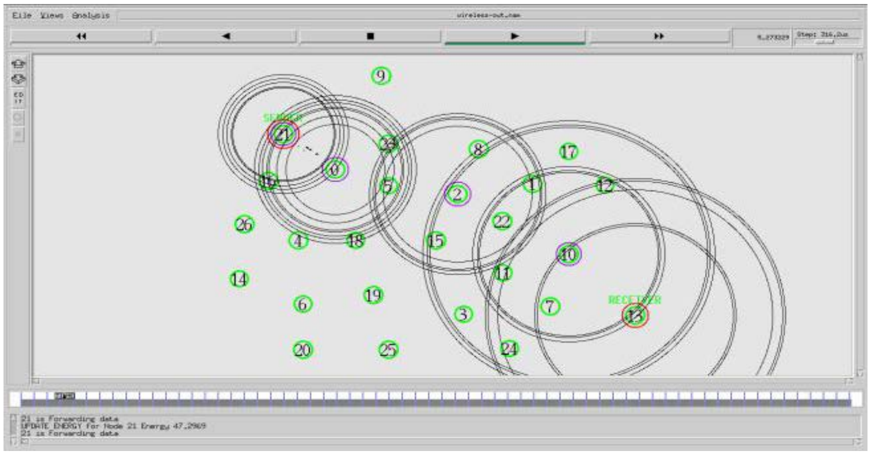
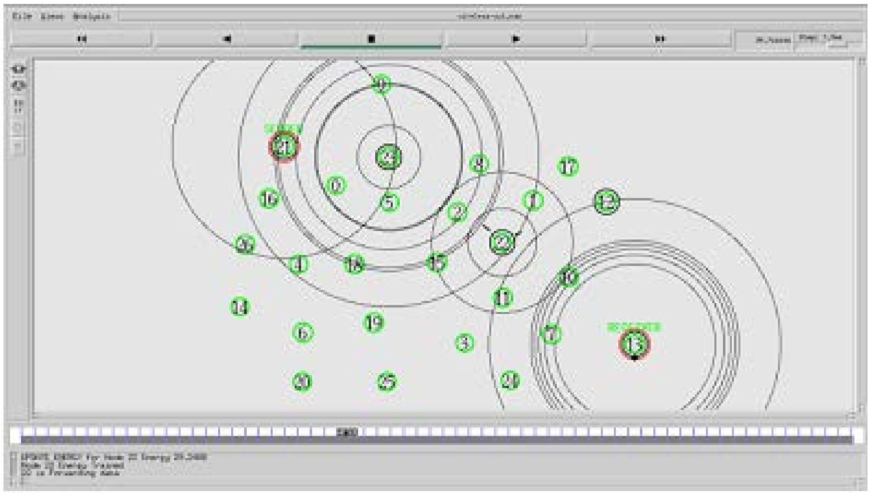


Fig. 1: 21 node as sender and node 13 as receiver. Communication takes place between 21 and 13 with route 21→0→2→10→13



```
21 is Forwarding data
UPDATE ENERGY for Node 21 Energy 47.2969
21 is Forwarding data
```

Fig. 2: Depicting the communication between the sender and receiver



UPDATE ENERGY for Node 22 Energy 29.2488
Node 22 Energy Traced
22 is Forwarding data

Fig. 3: Depicting the new route 21→23→22→12→13

All the middle nodes represented as a blue circle surrounding them. When the energy of a specific node down to 18, the AODV evades that specific node. Here, in thus, the nodes with energy <18 (nodes 0, 2, 10) are neglected using this algorithm as assuming these nodes to be malicious. In real time a malicious node will groove its energy earlier than that of the normal nodes (Fig. 3) (Borgia *et al*., 2006; Jain *et al*., 2009; Kettaf *et al*., 2006).

## CONCLUSION

In this study, a new technique "CBDET" is proposed for detection and isolation of malicious nodes in "MANETs" using cross-layer technology. The simulation results exposed that the proposed mechanism successfully work as expected while using "AODV" protocol. The residual energy of nodes was calculated and the identified of malicious nodes method is based on threshold value. Once the node is detected as malicious the node is isolated from the network by dropping "RTR" packets. AODV protocol become automatically selects a new route.

## REFERENCES

Babu, K.S. and K.C. Sekharaiah, 2013. Securing AODV with authentication mechanism using cryptographic pair of keys. Intl. J. Comput. Sci. Inf. Secur., 11: 42-45.

Borgia, E., M. Conti and F. Delmastro, 2006. Mobileman: Design, integration and experimentation of cross-layer mobile multihop ad hoc networks. Commun. Mag. IEEE., 44: 80-85.

Gopinath, S., D .S. Nirmala and N. Sureshkumar, 2012. Misbehavior detection: A new approach for MANET. Intl. J. Eng. Res. Appl., 2: 993-997.

Jain, J., M. Fatima, R. Gupta and K. Bandhopadhyay, 2009. Overview and challenges of routing protocol and MAC layer in mobile ad-hoc network. J. Theor. Appl. Inf. Technol., 8: 6-12.

Kettaf, N., H. Abouaissa, T. Vuduong and P. Lorenz, 2006. A cross layer admission control on-demand routing protocol for QoS applications. Int. J. Comput. Sci. Network Secur., 6: 98-105.

Li, W. and A. Joshi, 2008. Security issues in mobile ad hoc networks-a survey. Master Thesis, Department of Computer Science and Electrical Engineering, University of Maryland, College Park, Maryland.

Rachedi, A. and A. Benslimane, 2009. Toward a cross-layer monitoring process for mobile Ad hoc networks. Secur. Commun. Networks, 2: 351-368.

Rajaram, A. and D.S. Palaniswami, 2009. A trust based cross layer security protocol for mobile Ad hoc networks. Intl. J. Comput. Sci. Inf. Secur., 6: 165-172.

Suresh, K.B. and K.S. Chandra, 2008. Mobile Ad-Hoc networks: A novel survey. Proceedings of the International Conference on Advanced Computing and Communication Technologies for High Performance Applications Vol. 1, September 24-26, 2008, Federal Institute of Science and Technology, Angamaly, India, pp:262-269.