International Journal of Computing and Corporate Research
ISSN (Online) : 2249-054X
Volume 4 Issue 1 January 2014
International Manuscript ID : 2249054XV4I1012014-06

A PRAGMATIC IMPLEMENTATION OF SECURITY BASED ALGORITHM IN MOBILE ADHOC NETWORKS

Rajinder Singh
Research Scholar
Deenbandhu Chhotu Ram University of Science & Technology
Murthal, Haryana, India

Dr. Parvinder Singh
Associate Professor
Department of Computer Science and Engineering
Deenbandhu Chhotu Ram University of Science & Technology
Murthal, Haryana, India

Dr. Manoj Duhan
Chairman
Department of Electronics and Communications
Deenbandhu Chhotu Ram University of Science & Technology
Murthal, Haryana, India

ABSTRACT

Mobile Ad-hoc Network is the moving hub as opposed to any altered foundation, go about as a versatile switch. These mobile switches or points are in charge of the system versatility. The

International Journal of Computing and Corporate Research
ISSN (Online) : 2249-054X
Volume 4 Issue 1 January 2014
International Manuscript ID : 2249054XV4I1012014-06

historical backdrop of portable system start after the development of 802.11 or WiFi they are for the most part utilized for uniting among themselves and for joining with the web through any settled foundation. The automobile systems including auto, transports and trains outfitted with switch goes about as settled Mobile Ad-hoc Network. The systems in motion today comprises numerous inserted gadgets like form in switches, electronic gadgets giving web association with it gives, data and infotainment to the clients. These advances in MANET helps the vehicle to speak with one another, at the time of crisis like mishap, or amid climatic changes like snow fall, and at the time of road obstruction, this data will be educated to the adjacent vehicles. In the present days, the advances climbing to give proficiency to MANET clients like giving enough storage room, as we all know the distributed computing is the cutting edge processing standard numerous scrutinizes are leading tests on Mobile Ad-hoc Network to give the cloud benefit safely. This paper endeavors to propose and execute the security based algorithmic approach in the versatile adhoc systems including different types of attacks.

Keywords : MANET, Network Security, Wormhole Attack, Secured Algorithm

INTRODUCTION

A mobile ad hoc network (MANET) refers to the continuously self-configuring, infrastructure-less network of mobile devices connected without wires. Each device in a MANET is free to move independently in any direction, and will therefore change its links to other devices frequently. Each must forward traffic unrelated to its own use, and therefore be a router. The primary challenge in building a MANET is equipping each device to continuously maintain the information required to properly route traffic. Such networks may operate by themselves or may be connected to the larger Internet. They may contain one or multiple and different transceivers between nodes. This results in a highly dynamic, autonomous topology

In case a mobile node wants to communicate with another mobile node which is too far from the source node, it should depend on relay node as bridge to communicate with destination. Relay

node is nothing but another mobile node. In this case there arises a question of security. Apart from authentication, reliability and acceptance it should also aware of the address location and packet traffic digression. In this manuscript we are going to concentrate on the various issues that affect the ad-hoc networks security mechanism and also we are going to concentrate on pros and cons of Mobile networks protocols. We are also concentrating on enhancing security and reliability to Mobile Ad-hoc Network (MANET). Many researches were done before to provide security to MANET but none of the protocol shines in providing security and performance. There are many defects in the Mobile framework; this may cause unknown nodes to connect frequently without any proper routing. In order to prevent other nodes from trespassing we are going to concentrate on providing more security to Mobile Ad-hoc network.

BLACK HOLE ATTACK

Black hole attack is the serious problem for the MANETs, in this problem a routing protocol has been used by malicious node reports itself stating that it will provides shortest path. In flooding based protocol, a fake route is created by the malicious node rather than the actual node, which results in loss of packets as well as denial of service (DoS).

International Journal of Computing and Corporate Research
ISSN (Online) : 2249-054X
Volume 4 Issue 1 January 2014
International Manuscript ID : 2249054XV4I1012014-06

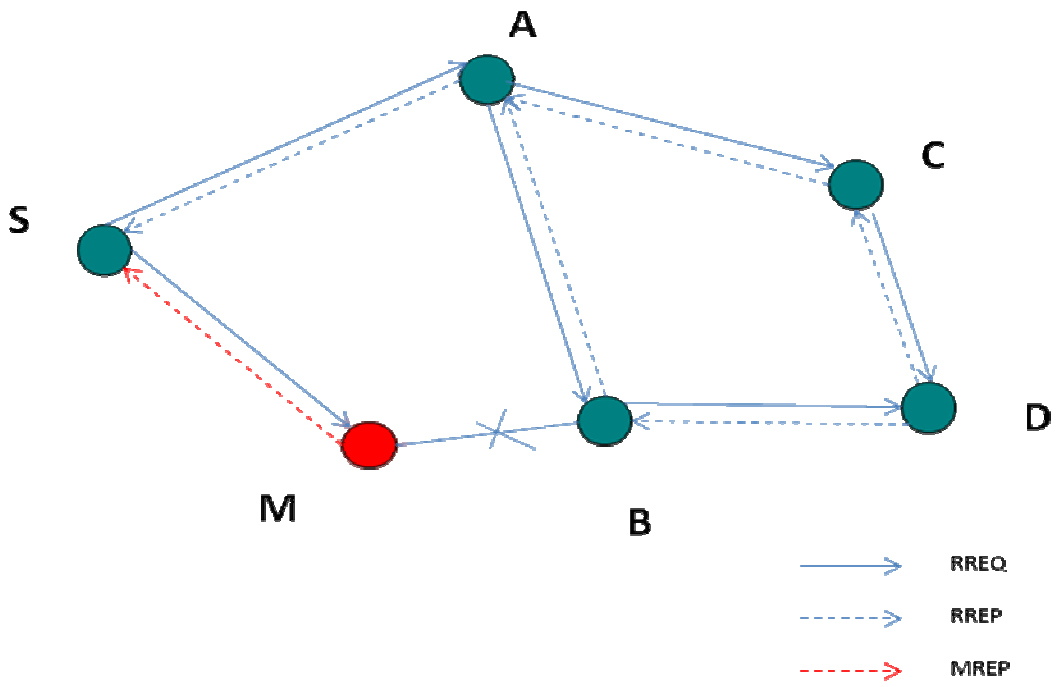


Figure 1 - Black hole attack

In the figure, S and D nodes are the source and destination nodes, A B C are the intermediate nodes and M is the malicious node. RREQ and RREP are the key terms for route request and route reply respectively. MREP is abbreviation for malicious reply.

CLASSICAL TECHNIQUE

Two tier secure AODV (TTSAODV)

TTSAODV protocol is proposed earlier to prevent the black hole attack. In these protocol two levels of security is provided

1. During route discovery mechanism and
2. During data transfer mechanism

In this technique, black hole attack is easily identified either of these two techniques, even it fails in any of the mechanism. The major drawback in this technique causes enormous packet loss and delay in transferring packet.

Resource consumption attack

In the resource consumption attack, a malicious node can try to consume more battery life demanding too much of route discovery, or by passing unwanted packets to the source node.

Location disclosure attack

In the location disclosure based attack, the malicious node collects the information of routes map and then focus on further attacks. This is one of the unsolved security attacks against MANETs.

Multi layer attacks in MANET

There are different types of multilayer attacks in MANET, they are as follows

- Denial of Service (DoS)
- Jamming
- SYN flooding
- Man In Middle attacks
- Impersonation attacks

Denial of service (DoS) attacks

In this type of attacks, the attacker injects enormous amount of junk packets into the network which leads to the loss of network resources and causes congestion among the wireless networks.

Prevention mechanism

The prevention mechanism divides into two categories

- Local and

- Global

Local solution

Protection of individual nodes involves three categories

- Local solutions
- Changing IPs
- Creating client bottle neck

Local router solutions

By installing the filter on the local router to detect the infiltrating IP packets is stopped using time worn short term solutions.

Changing IP Address

By changing the victims IP address is one of the techniques to prevent the attacker from accessing its network, however this technique is not effective, many attacker node will easily identify the newer IP address.

Creating Host bottle neck

The major objective behind this technique is creating bottle neck process on the zombie computers, for example making simple puzzle to solve before establishing connection or a software already installed in host computer asks to answer random question whenever attacker computer try to establish connection. The local solution consumes some time to perform connection this is unacceptable drawback.

Jamming

Jamming is known as the DoS attack that affect communication between two nodes, the main goal of jamming is to block the valid user's like sender and receiver from transmitting and receiving packets, jamming is divided into two types

- Physical jamming attacks

International Journal of Computing and Corporate Research
ISSN (Online) : 2249-054X
Volume 4 Issue 1 January 2014
International Manuscript ID : 2249054XV4I1012014-06

- Virtual jamming attacks

Physical jamming

Physical jamming is caused by continuous transmission of packets to the receiver or by causing packet collision at the receiver. Physical jamming is also known as radio jamming, radio jamming is simple attack causing more disrupt to the authorized users. Jammers causing this attack block the authorized users from accessing the wireless channel by controlling the wireless medium.

The nodes trying to communicate strangely waiting for the carrier sense timing of the channel to become idle. This put the nodes into list of larger exponential back off period.

Virtual Jamming

Virtual jamming is most often possible at the MAC (Medium Access Control) layer, causing affects on Rate to send (RTS) frames, or Clear to send (CTS) frames, or data frames. One of the advantage of this attack is it consumes less power than comparing to physical or radio jamming.

In virtual jamming the malicious node try send RTS command continuously on the transmission with more number of times. In this process the malicious node blocks the transmission limited amount of power. This attack more dangerous than that of physical attack, by sending false frames it will disturb other node from accessing for certain period of time.

Existing techniques

To prevent and secure the network from jammer or from hidden attacker who causes the network jamming RTS and CTS method is implemented, this mechanism minimizes the attacker node from handshaking process.

Security measures against jamming in MANET

International Journal of Computing and Corporate Research
ISSN (Online) : 2249-054X
Volume 4 Issue 1 January 2014
International Manuscript ID : 2249054XV4I1012014-06

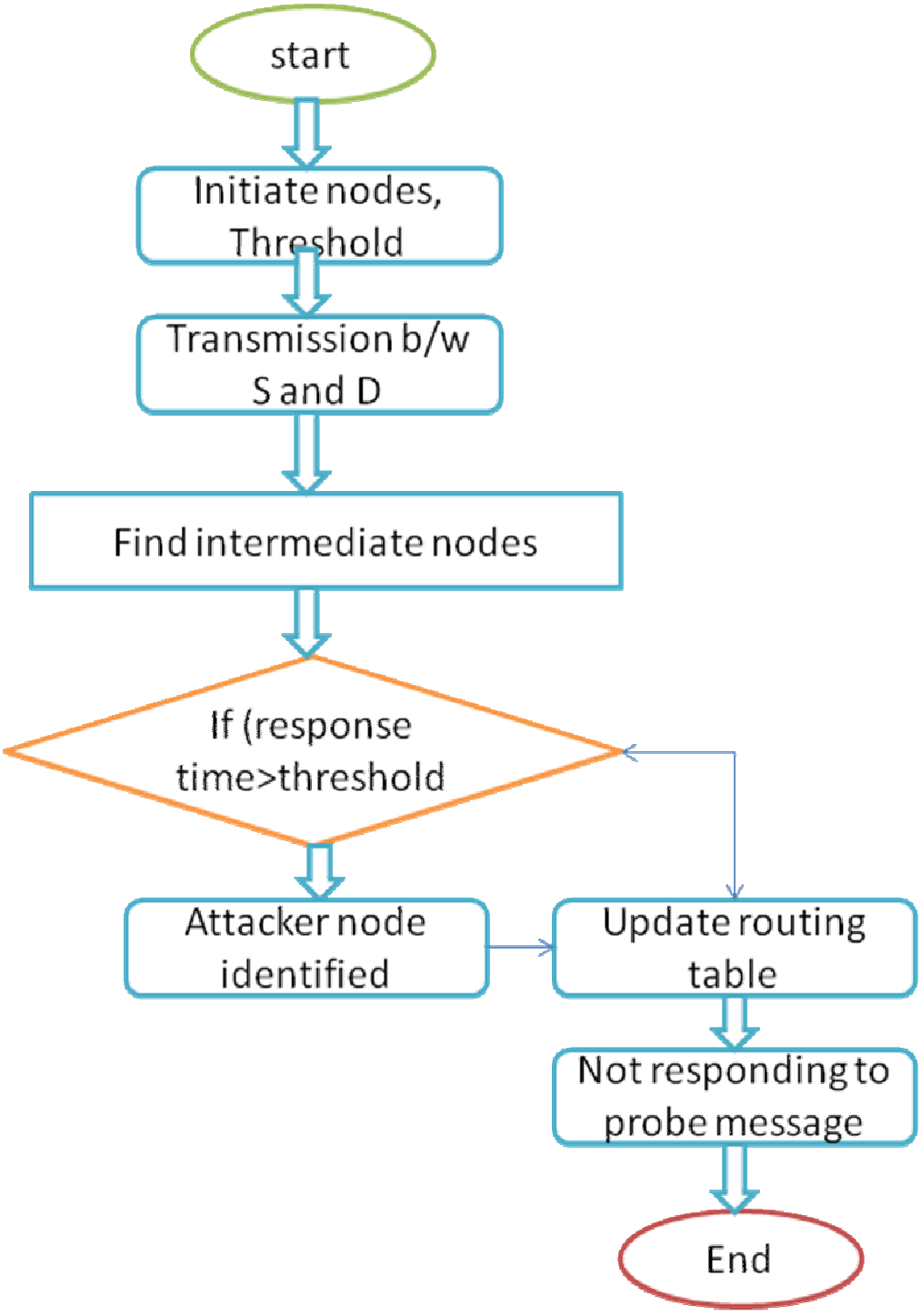


Figure 2 – Flowchart of Jamming attack

International Journal of Computing and Corporate Research
ISSN (Online) : 2249-054X
Volume 4 Issue 1 January 2014
International Manuscript ID : 2249054XV4I1012014-06

Swarm intelligence

Swarm intelligence is an artificial intelligence technique introduce by Beni and wang in 1989, in the perspective of cellular robotics, it is based about the study of combined behaviour of self organized systems.

Swarm intelligence is usually conjured of simple agents from a population interacting with each other locally. Basically there is no instructor to control the system how to perform, but this local instance lead to the global activities emergence.

Swarm intelligence types

There are two basic swarm intelligence types namely

- Ant colony optimization
- Atom swarm intelligence

Ant colony optimization

A complex task cannot be performed by a single ant, but a group of ants can make even a complex task into simpler ones. Ant colony optimization technique is used to provide fair resolution to the various optimization problems. In this optimization technique moving man-made ants are really helpful in providing solutions by impersonating the real ants, dump fake pheromone on the graph so that the future man-made ants can provide even better solution to these problems.

Implementation of ant colony optimization algorithm

In an ant colony, the ants sorted their foods and larvae in consistent heaps. There are several steps helpful solving the optimization problems in MANET.

- The platform is a two dimensional lattice
- The mobile nodes are sprinkled on the lattice

International Journal of Computing and Corporate Research
ISSN (Online) : 2249-054X
Volume 4 Issue 1 January 2014
International Manuscript ID : 2249054XV4I1012014-06

- The artificial ants are developed in such a way that automatically leap from one node to the another node
- Each and every node has ability to change the colour of the mobile node in accordance with the perspective rules.
- This perspective rule requires only local values as the input.

The mobile nodes are coloured, re-coloured or made colourless by a mechanism which take local data as an input. The constriction on colouring the node depends on type of node and its cluster capability.

The **probability** $P(d)$ of discolouring a mobile node A, is denoted as follows

$$P(d) = (Cd/(Cd + fa(x)))^2$$

x=number of exclusive neighbour

Cd=constant

$fa(x)$=local density function related to node A

The **probability** $P(r)$ of re colouring a mobile node A, increases with number of similar coloured nodes in the neighbourhood.

$$P(r) = (fa(x)/(Cr + fa(x)))^2$$

Cr=constant

$fa(x)$=local density function related to node A

The probability of untouched nodes $P(U)$

$$P(U) = 1 - (P(d) + P(r))$$

It is used to estimate the traffic overhead of the mobile node A.

Pseudo code for atom swarm intelligence algorithm

Declare $w, C1, C2,$ max_iterations, target_suitability, $Lmin, Lmax, vmin$ and $vmax$

FOR each atom A

International Journal of Computing and Corporate Research
ISSN (Online) : 2249-054X
Volume 4 Issue 1 January 2014
International Manuscript ID : 2249054XV4I1012014-06

FOR each dimension d

Declare Location randomly, $Lmin \leq Lid \leq Lmax$

Declare Velocity vid randomly, $vmin \leq vid \leq vmax$

End FOR

END FOR

Iteration i=0

DO

FOR each atom A

Calculate suitability (A)

IF suitability (A) > suitability $(ptopid)$

FOR each dimension d

$ptopid = Lid$

End FOR

END IF

IF suitability (A) > suitability $(mtopd)$

FOR each dimension d

$mtopd = Lid$

End FOR

END IF

END FOR

FOR each atom A

FOR each dimension d

Compute velocity according to the equation

$$vid(i+1) = w.id(i) + C1.random.(ptopid - Lid) + C2.random(mtopd - Lid)$$

Update atom position as per equation

International Journal of Computing and Corporate Research
ISSN (Online) : 2249-054X
Volume 4 Issue 1 January 2014
International Manuscript ID : 2249054XV4I1012014-06

$$Lid(i+1) = Lid(i) + vid(i+1)$$

Confine vid within $vmin$ and $vmax$

Confine $Lid$with $Lmin$ and $Lmax$

END FOR

END FOR

i=i+1

WHILE i $\leq$ max_iterations AND suitability $(mtopd) \prec$ target_suitability

Proposed Algorithm to prevent Black hole attack

In this proposed algorithm, the Expected broadcast count algorithm is introduced. With the help of this algorithm highest throughput is possible between the nodes but however the actual algorithm does not prevent the black hole attack.

Throughput refers to the average number of message transmitted in a given time, it is usually measured in bps or bits per second, and it is also mentioned as packet delivery ratio. Malicious node plays a major role in affecting throughput in black hole attacks.

Secure mesh network measurement technique is proposed in this project to prevent the black hole attacks during route discovery process between the source and destination node with the help of the throughput measurement values, this makes the routing process more consistent and efficient communication between the nodes.

Pseudocode DoS prevention algorithms

BEGIN

Manage_constraint_check (node n, Data Unit d)

FOR each p in n DO

International Journal of Computing and Corporate Research
ISSN (Online) : 2249-054X
Volume 4 Issue 1 January 2014
International Manuscript ID : 2249054XV4I1012014-06

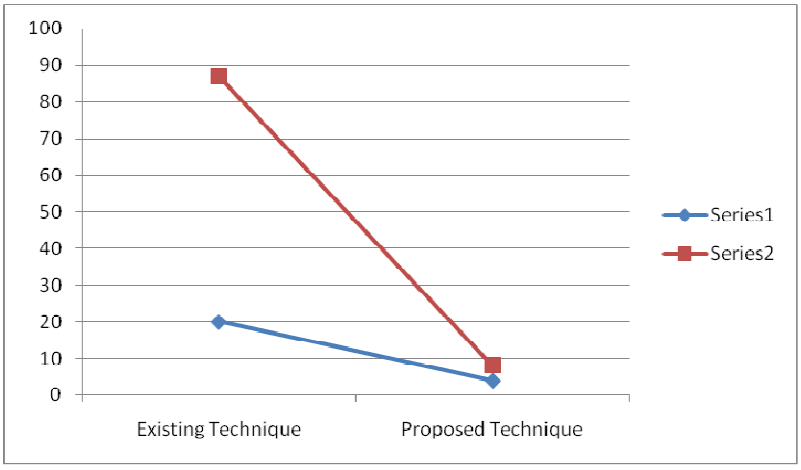
Manage_update (path p, Data Unit d)

END FOR

END

Table 1 – Comparison of Packet Loss in Existing and Proposed Approach

	Existing Technique	**Proposed Technique**
Packet Loss : Scenario 1	20	4
Packet Loss : Scenario 2	87	8



International Journal of Computing and Corporate Research
ISSN (Online) : 2249-054X
Volume 4 Issue 1 January 2014
International Manuscript ID : 2249054XV4I1012014-06

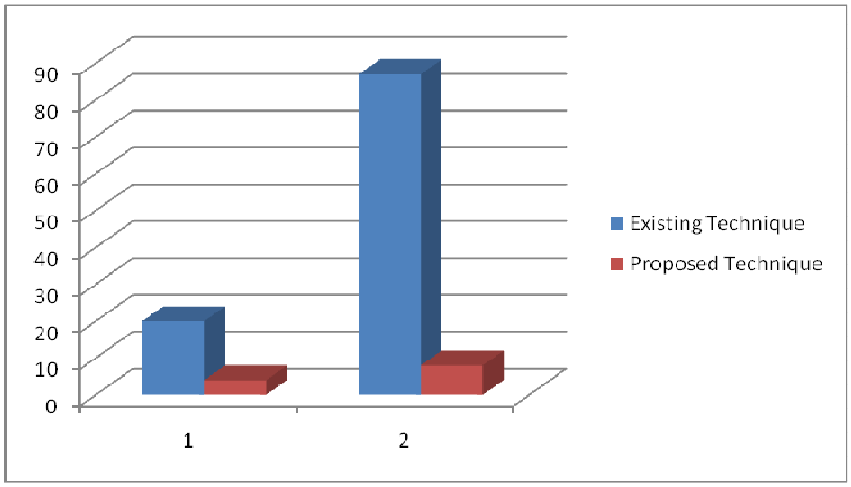


Figure 3 - Comparative Analysis of Proposed and Existing Approach

CONCLUSION

This paper underlines various aspects and dimensions of the attacks in mobile ad hoc networks. In this paper, the process and execution to avoid the ddos and black hole attacks are implemented using the novel algorithm. In this research task, the future work can be implemented with the use and integration of simulated annealing that is one of the prominent metaheuristic for the combinatorial optimization problems.

REFERENCES

[1] Karaboga, Dervis, and Bahriye Akay. "A survey: algorithms simulating bee swarm intelligence." *Artificial Intelligence Review* 31, no. 1-4 (2009): 61-85.

[2] Sowmya, K. S., T. Rakesh, and P. Hudedagaddi Deepthi. "Detection and Prevention of Blackhole Attack in MANET Using ACO." *International Journal of Computer Science and Network Security* 12, no. 5 (2012): 21-24.

[3] Baras, John S., and Harsh Mehta. "A probabilistic emergent routing algorithm for mobile ad hoc networks." In *WiOpt'03: Modeling and Optimization in Mobile, Ad Hoc and Wireless Networks*, pp. 10-pages. 2003.

[4] Jiang, Tao, and John S. Baras. "Ant-based adaptive trust evidence distribution in MANET." In *Distributed Computing Systems Workshops, 2004. Proceedings. 24th International Conference on*, pp. 588-593. IEEE, 2004.

[5] Singh, Gurpreet, Neeraj Kumar, and Anil Kumar Verma. "Ant colony algorithms in MANETs: A review." *Journal of Network and Computer Applications* 35, no. 6 (2012): 1964-1972.

[6] Asokan, R., A. M. Natarajan, and C. Venkatesh. "Ant based dynamic source routing protocol to support multiple quality of service (QoS) metrics in mobile ad hoc networks." *International Journal of Computer Science and Security* 2, no. 3 (2008): 48-56.

[7] Mehfuz, Shabana, and M. N. Doja. "Swarm intelligent power-aware detection of unauthorized and compromised nodes in MANETs." *Journal of Artificial Evolution and Applications* 2008 (2008): 3.

[8] Goel, Aditya, and Ajaii Sharma. "Performance analysis of mobile Ad-hoc network using AODV protocol." *International Journal of Computer Science and Security (IJCSS)* 3, no. 5 (2009): 334-343.

[9] Prasad, Sunita, Y. P. Singh, and C. S. Rai. "Swarm based intelligent routing for MANETs." *International Journal of Recent Trends in Engineering* 1, no. 1 (2009): 153-158.

[10] Saleem, Kashif, Norsheila Fisal, S. Hafizah, S. Kamilah, and Rozeha A. Rashid. "Ant based self-organized routing protocol for wireless sensor networks." *International Journal of Communication Networks and information security (IJCNIS)* 1, no. 2 (2009).

[11] Suguna, S. Kanimozhi, and S. Uma Maheswari. "Comparative Analysis of Bee-Ant Colony Optimized Routing (BACOR) with Existing Routing Protocols for Scalable Mobile Ad Hoc Networks (MANETs) based on Pause Time." *IJCSNS* 12, no. 4 (2012): 10.