International Journal of Engineering & Technology, 7 (2.19) (2018) 75-79

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research paper

Enhanced AODV Protocol to Secure Routing in MANET with Optimization Techniques

V. Keerthika [1]*, Dr. N. Malarvizhi [2]

[1] *Research Scholar,*
Department Of Computer Science And Engineering, School Of Computing,
Vel Tech Rangarajan Dr. Sagunthala R&D Institute Of Science And Technology,
Avadi, Chennai-600 062, Tamil Nadu, India.
[2] *Professor & Head,*
Department Of Computer Science And Engineering, School Of Computing,
Vel Tech Rangarajan Dr. Sagunthala R&D Institute Of Science And Technology,
Avadi, Chennai-600 062, Tamil Nadu, India.
Drnmalarvizhi@Gmail.Com
** Keerthivenkatt@Gmail.Com*

Abstract

Mobile Adhoc Network is the infrastructure less network. Routing in MANET is the process of information or the packets transmission to the destination node from the source. The routing protocol controls the data flow in any network, it will make efficient to reach its destination. Most protocols are vulnerable to attacks in open media communications and wide are distribution. Since we are in need of better routing protocols are needed for an efficient data transmitting to improve the MANET features. In this paper, we proposed enhanced AODV routing protocol using ABC optimization algorithm to provide secure Routing in MANET. The simulations carried out in NS2 are provided to demonstrate the performance using parameter threshold, throughput, packet success rate, computational overhead, routing overhea .

Keyword:*AODV,WTABC,MANET,PDR* *:*

1. Introduction

In the fast few decades among all the contemporary wireless network MANETs one of the most important and unique application, nodes communicate directly with each other when in the same range [7]. Due to the characteristics of mobility and scalability it is widely used in mission applications. In this communication module, major problem is occurring when the node's distances are beyond the limit and it leads the communication error. This problem can be solved by allowing the intermediate nodes. Secure data transmission is a critical issue in networks of any type Wireless sensor Network, MANET. Adhoc network are very flexible and reach and each type of communication among two nodes .The nodes can leave and join any time to the network to improve the service. Hence it leads to enter some malicious nodes which makes MANET vulnerable to attack.

1.1 Routing in MANET

In MANET the most popular approach is on-demand Routing. Instead of periodic update of routing message, route table, model of network we can use on-demand protocol for dynamic process. The routing protocols divide into hybrid, Table drive, on demand routing protocols, for the quick data transmission we need routing protocols that adopts topology changes. Routing protocol is used to data transport in MANET . The properties of routing protocols

- The routing protocols must provide multiple path to destination.
- Provide loop free path to destination
- Provide node disjoint path to destination

Table 1 Routing protocols

Table driven protocols/proactive	**On demand protocols/reactive**
Information available immediately from route table	After route discovery
Predicate advertisement of route update	Only when request
Depends on the size of network	Depends on the communicating nodes

In recent years, MANET routing protocol is playing vital role in Information and Communication Technology (ICT), which is constructed with Proactive, Reactive and Hybrid layers. Proactive is used to manage the routes and routers other nodes in a network. Reactive node is playing on the data delay which cause the data reducing. Besides, hybrid layer is the combination of proactive and reactive which serves inner network and outer network respectively. Most of the Researchers are concentrating the routing protocols how they will be secured. In this network, Passive and active attacker are entering easily to damage the network or dilute the system. Passive the attackers snooping the network with IP and delay the work flow of the networking system. Active attackers play the role of Denial service. We concentrate about this model will be secure and reduce the delay between the nodes. Many algorithm are proposed to efficient and reliable routing maintenance

Adhoc On-Demand Distance Vector (AODV) is having the message format which demonstrates the RREQ, RREP and RERR. RREQ (Route Request) is used to send the packets to the connected nodes within the network and check the valid path. RREQ (Route Reply) is depicting the one – to one communication with secured process. RERR (Route Error) is occurred when the network model has been changed.
The AODV will use the fields mentioned below for Route Table is entries.

- IP address of the destination
- The Seq_Num of DEST
- Flag id of DEST and STATE
- Network INTF
- Counts – HOP and forth coming HOP

2. Black-Hole Attack

In this attack, unwanted node has been addressed with fake route information which is communicating from RREP. As per Adhoc module, RREP is activating with false data and malicious node thrown away the packet instead of the forward process.

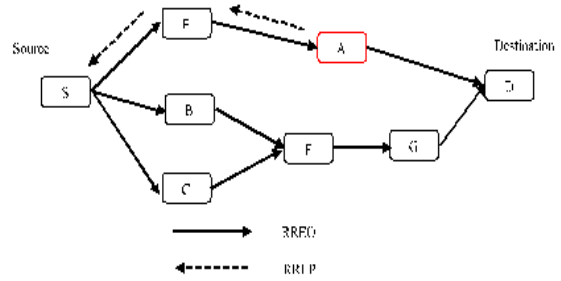

Figure 1 Black Hole Atttack on AODV routing

Figure 1 tells the way of black hole attack in the network. For instance, transfer between Source S and Destination D, S sends the request to E, B, and respectively. Eventually malicious path which contains A replied immediately. After data transmitting it won't forwarding, even though another two valid paths are available. In this processing, our highlighting point is malicious node A responding rate is high.

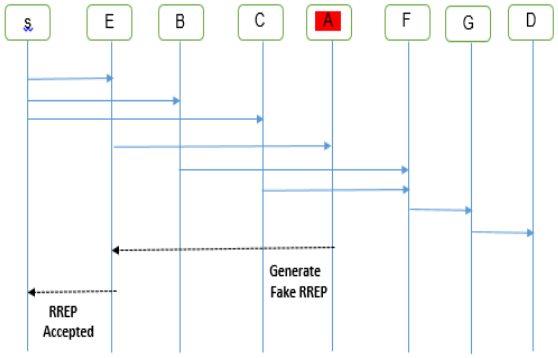

Figure 2. Malicious node in S and D with discovering track

Swarm intelligence is the self-possessed interactive agents or singles. It is motivating the concept of intelligent behavior with self-organization and division of labor. Self-organization, which is consisting of basic rules to interact with the components in a system each other. It is following feedback effects with true and untrue parameters and more numbers of interfaces. Division of labor deals with multiple task performed by an agent. This agent can makes the changes in the searching domain or networ**k.** This optimization algorithm is coining the intelligence forging behavior of bees with its swarming have been successfully used in route technique.

3 .Related Work

Jaspal Kumar et al .[1] designed the work the damage of AODV when black hole node present has been evaluated and solution to defend against the problem has been proposed to prove its efficiency .The packet process of normal AODV is improved to detect routing misbehavior and alert other nodes using default AODV control message, HELLO messages to reduce additional overhead.

Neelam khemariya & Ajay Khuntetha [2] , used the efficient algorithm which can detects two types attack called single Black hole attack and the Cooperative Black hole attack.

Dervis karboga [3] specifies the work. In this research work the ABC is used for optimization ,results compared with Genetic Algorithm(GA),Particle Swarm Algorithm(PSO), the results shows that ABC out performed the other algorithms
Devis Karboga [4] performed a work, ABC used to test huge set of numerical test functions and the results given using by ABC Algorithm is compared with existing, the performance proves that this meyhod is better performed than other algorithm.
Arti , deepika [5], Proposed algorithm Which can avoid network congestion and then it can prolong the life cycle of the whole network and optimizes the routing paths to transfer the data in WSN ,ABC is also proposed to optimization. Ali Ahmed [6] implements an ant algorithm with comparison of routing protocols and to reduce the E2E delay .
D.Jinil persis ,T.paul Robert [7] presented a multi objective AODV (MOAODV) algorithm, performed well in larger Network which uses the estimated objective vector using the parameters delay, hop distance ,load, cost could traverse from source to destination. Their performances in the various scenarios are then compared to reflect the relative merits of each protocol.
Alkin and Eral Eme[13] Proposed (ABC-SA)approach, instead of employing a single search mechanism throughout the search process, a probabilistic multisearch mechanism with three different search rules is used. A probabilistic selection is employed using predefined probability parameters to select the search rule within both employed and onlooker bee phases.

4. Methodology

We demonstrated the optimum routes with consistent effects of results through the proposed method WTABC. The forging behavior of swarm are suitable for solve routing problem in MANET. A perfect network is called without malicious and won't drops any packet within the network. The trust node is nominated by the parameters of authentication and certification which are expressed by the other nodes. The problem is unable to detect in case a malicious node authenticate itself but after periodic time it behaves the unwanted functions like BH attack.

4.1 Trust Computation

The trust model of TAODV protocol has the process of trust updation ,trust routing, trust recommendation
Trust computation by existing Method

Algorithm

1. Monitor the next hop transmission
2. If the next hop forwards packets
3. If (Source address of forwarded packet == source address sent by monitor)
   3.1 If (destination address of packet== destination address of original packet) then reward the next hop as Trust
   3.2 Else detect node as malicious ensuring black hole attack

In this work the AODV protocol [12] is considered along with trust calculation. The communication of nodes ,based on the trust level with its neighbors. Most reliable node will have the high

level of trust value. A node is collecting its neighbor opinion based on the direct trust ,In this work AODV is modified to compute both direct and indirect trust .

$$T=w_1 \times MR + w_2 \times LQ + w_3 \times SD$$

Where , MR=Malicious Route reply,

LQ=link quality,

SD= Successful Delivery

The Indirect Trust IT is computed based on the packets dropped by a node , The Direct Trust DT is computed based on the packets forwarded by a node , the total trust is computed by

$$T_{total} = IT + DT$$

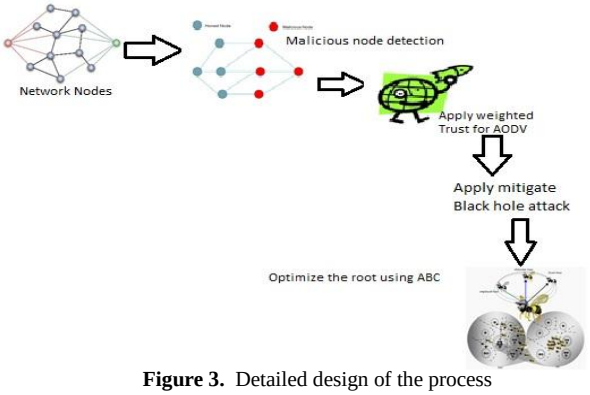

Figure 3. Detailed design of the process

4.2 Artificial Bee in Proposed Work

1. Select source and destination in network, where destination associated with food source
2. Generate artificial bee at random nodes, intermediate nodes are worker bees
3. Transfer the data using AODV routing protocol based on trust node ,an employee bee refresh the packet in a periodic manner
4. Scout bee search for black hole node
5. Employee bee optimize the route

5. Experimental Setup

The simulation of proposed work is conducted in the following experimental setup.

Table 3. Components of Simulation

Parameters	Setting
Routing Protocol	AODV
Transmission range	200m
Packet size(bytes)	512 byte
Transmission rate	5 packets/sec
Nodes speed	25 m/s
Simulation time	800 s
Number of nodes	50
Map size	1000 m *1000 m
Maximum Malicious nodes	15 nodes
Movement Model	Random
Types of attack	Black hole attack
Traffic Model	Constant Bit Rate

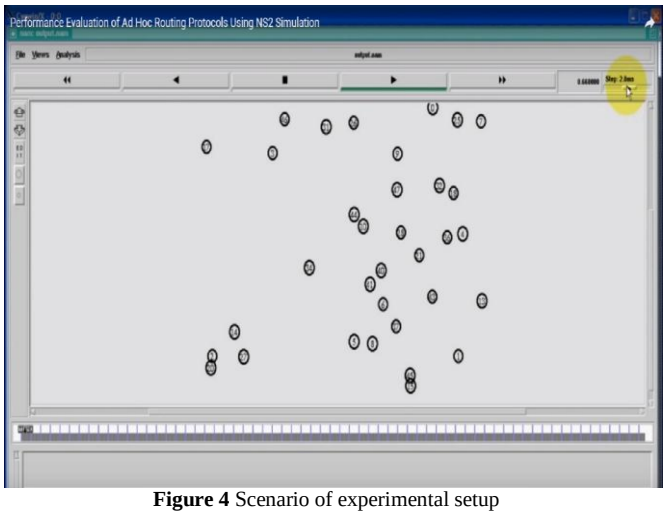

Figure 4 Scenario of experimental setup

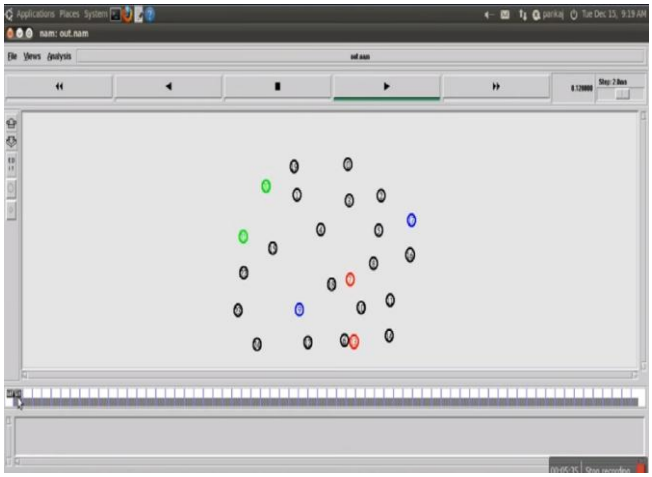

Figure 5. Malicious Node Detection

Table 4 ABC parameter setting

Parameter	values
Colony size	50
Maximum no of cycle	500
Number of employed bees	50%
Number of onlooker bees	50%
Scout bees	1

6. Result and Discussion

Various parameter used for analysis are described below

Throughput**:** It is used for performance metrics that how much data has been transferred in a stipulated time bounds. Usually it is referred as Bits or packets in various size parameters.

Throughput= P_Size (E_Time – S_Time) * 0.008 (Process in thousands)

Packet Delivery Ratio(PDR) : It identifies the transferred packets from source to destination with packet numbers.

PDR= (R_PKTS / Gen_PKTS)*100

DELAY: Eventually delay is referring the time between the initiating the process with completion of the process (like data transfer, signal transmission)

The Table 5 shows the performance analysis the existing and proposed method of packet delivery, throughput

Table 5 Evaluations of performance in existing method

Nodes	Gen_PKTS	R_PKTS	PDR	Throughput
5	224	192	85.71429	222.464
10	244	212	86.88525	242.304
15	264	238	90.15152	262.096
20	284	257	90.49296	281.944
25	382	335	87.69634	379.32
30	412	374	90.7767	409.008
35	602	542	90.03322	597.664
40	885	764	86.32768	878.888
45	1024	928	90.625	1016.576
50	1064	928	87.21805	1056.576

Table 6. ABC method for performance evaluation in proposed method

Nodes	Gen_PKTS	R_PKTS	PDR	Throughput
5	2164	2100	97.04251	1369.73
10	2185	2104	96.29291	1369.43
15	2276	2160	94.90334	1372.43
20	2367	2271	95.94423	1336.28
25	2388	2355	98.61809	1335.98
30	2408	2271	94.31063	1386.75
35	2620	2539	96.9084	1398.75
40	2822	2651	93.94047	1543.36
45	2882	2722	94.4483	1546.87
50	2972	2881	96.93809	1547.47

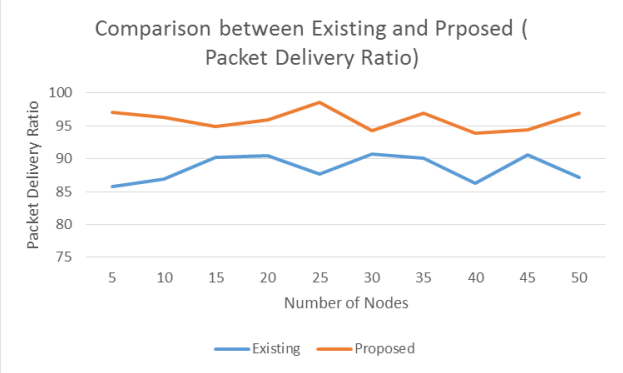

Figure 6 comparison chart of PDR of Existing and proposed

The simulations are runs 10 times and the average value is tabulated in table 5 and ,6 from the figure 6 can observed that the proposed ABC method outperforms better than existing method based on the parameter Packet Delivery Ratio.

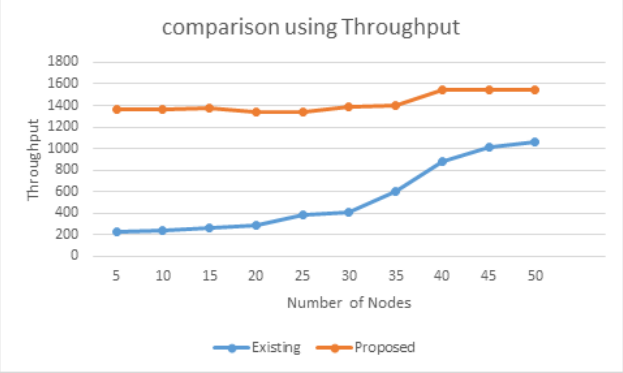

Figure 7 comparison chart of Throughput of Existing and proposed

The simulations are executing ten times with emits of mean value has been tabulated in table 5 and 6. In figure 7 shows the ABC optimizing techniques and inculcates how it is the best from the existing.

7. Future Work

We intend to elevate our simulations which are already mentioned in this paper. Then it should be the fully implemented ABC supported AODV protocol module. This will leads truthful and optimistic protocol. In future work, missing packets or pending packets are to be stored in the ADOV memory with necessary routing table information. This information will tell us how long the packets are residing in the memory and shown the actual problem also. Feedback applications are to be implemented for local transactions and disconnect the further operations. We will concentrate more on the buffering because intermediate nodes are to be controlled and monitored.

In future, we should contribute to demonstrate the role PERR system and its error messages. Besides it should be redefined and highly dynamic. We should improve the throughput metrics and less latency between the discovery routes

8. Conclusion

Since the contemporary wireless communication and mobile networking tools are vital for younger generation. We have to pave the execution of MANET protocols for smoother function. AS we discussed earlier, each protocol confines advantages and disadvantages. Besides those protocols are applicable, if the situation is needed for the mandatory protocols. By the result and discussion MANET is basically insecure by its nature. We supposed to maneuver the transactions through the MANET by using secured techniques like trustworthy optimization, black hole avoidance and so on. In this paper, we demonstrated theme not exclusively finds nevertheless eliminates the malicious node by segregating it. Finally it confined as safety and secured communication path.

The use of MANET has amplified over the past era. The security components in MANET are the most vital thing for this contemporary scenario. In previous security issues are playing only on cryptography and authentication techniques or trustworthy path mechanisms. Most of the researchers are concentrating only on improve the security ness and improving the path selection speed up techniques. Through our work, we may carry over our research work into attack the malicious node or path in the network form. By using ABC algorithm, not only mitigating the path it will find the malicious and remove malfunction from the node. Before transferring the data, the Sender should know the optimum path and how many malicious are to be detected and deleted. If the malicious is not able deleted, it will be transferred into quarantine section and analyze it.

References

[1]. Jaspal Kumar M. Kulkarni , Daya Gupta • S. Indu , " Secure route discovery in AODV in presence of blackhole attack " 2015

[2]. Neelam Khemariya & ajay " An Efficient algorithm for detection of Black hole attacke in AODV based MANETs ,*International Journal of Computer Applications (0975 – 8887) Volume 66– No.18, March 2013*

[3]. Dervis Karaboga Bahriye Basturk," A powerful and efficient algorithm for numerical function optimization: artificial bee colony (ABC) algorithm", J Glob Optim (2007) 39:459– 471Jul 2012.

[4]. Dervis Karaboga, Bahriye Akay," A comparative study of Artificial Bee Colony algorithm", Applied Mathematics and Computation 214 (2009) 108–132.

[5]. Arti , deepika "Path Optimization with Artificial Bee Colony Algorithm in WSN" ,IJETI International Journal of Engineering & Technology Innovations, Vol. 3 Issue 3, ISSN (Online): 2348-0866, www.IJETI.com ,may 2016

[6]. Ali Ahmed, "Modeling and simulation of a routing Protocol for ad hoc networks combining Queuing network analysis and ant colony Algorithms"-Dissertation-april-2005

[7]. Ellahadi M.Shasshuki,,Nan kang ,"EAACK-A secure intrusion Detection system for MANETs" IEEE transaction on Industrial electronics,Vol-60 N0-3 March 2013

[8]. Bhatia T, Verma AK (2013) Security issues in MANET: a survey on attacks and defense mechanisms. International Journal of Advance Research in Computer Science and Software Engineering 3(6):1382–1394

[9]. Vijay Chhari, Rajesh Singh, and S.S. Dhakad, " Enhanced and more secure AODV routing protocol to avoid black hole attack in MANET", IJCSNT, 2014.
[10]. Mou Zonghua , Meng Xiaojing. A modified AODV routing protocol based on route stability in MANET. Fourth IET International Conference on Wireless, Mobile & Multimedia Networks, pp. 63 - 67, 2011.
[11]. Chee-Wah Tan , S.K. Bose. Investigating Power Aware AODV for Efficient Power Routing in MANETs. Fifth International Conference on Information, Communications and Signal Processing, pp. 584 - 588, 2005.
[12]. M. Narayana1, L.Bhavani Annapurna2, K.Varalaxmi3," To Mitigate Wormhole Attack by using Trusted AODV with WAP -TSH methodology for MANET", International Journal of Engineering Science and Computing, November 2017, Volume 7 Issue No.11.
[13]. Alkin and Eral Eme, An Enhanced Artificial Bee Colony Algorithm with Solution Acceptance Rule and Probabilistic Multisearch , Computational Intelligence and Neuroscience ,2016