Received: January 6, 2018

International Journal of
Intelligent Engineering & Systems

http://www.inass.org/

An Efficient Detection of BH Attack with Secured Routing Using ACO and Dual-RSA in MANETs

Sunitha Mallasetty Shivamallaiah[1]* **Kwadiki Karibasappa[2]**

[1] *Dayananda Sagar College of Engineering, India*
[2] *Dayananda Sagar Academy of Technology and Management, India*
* Corresponding author's Email: gsunithaphd2017@gmail.com

Abstract: Nowadays, wireless communication plays a major role in sending information from one area to another in an effective way. In wireless communication, the important parameters are coverage area, power consumption, lifetime, and Black Hole (BH) detection in network with interconnected mobile nodes. Ant Colony Optimization (ACO) is used for finding shortest path in the Network. ACO helps in choosing another path, if there is any malicious node in the network. Data is secured using Dual Rivest-Shamir-Adleman (DRSA) technique and Black Hole Detection (BD) is used for identifying malicious node in the network. For efficient wireless system these parameters have been optimized, several algorithms have been applied to optimize the performance parameters and detect the BH in the network. Efficient BH identification with optimized routing algorithm is implemented in secured environment by using Dual RSA. The ACO-DRSA-BD algorithm precisely detected the BH Node (BHN) in finding the proper solution for data transmission using ACO and secured environment using DRSA. Hence, "ACO-DRSA-BD" finds proper solutions for transmitting data in the presence of BH Attacks and enhancing better performance parameters in terms of throughput, routing overhead and energy consumption.

Keywords: Black hole attack, Ant colony optimization algorithm, Dual Rivest-Shamir-Adleman.

1. Introduction

Mobile Ad-Hoc Network (MANETs) is one kind of self-configuring and dynamic wireless network, which is self-possessed of several portable user equipment. Mobile nodes communicate with each other without any fixed central base station to monitor the nodes and to transfer data between the nodes [1, 2]. Ant colony algorithm is an important category of metheuristic techniques, which can provide an efficient solution to many engineering problems [3]. However, there are still open issues about MANETs, for example, security issue, limited transmission transfer speed, damaging telecom messages, solid information conveyance, dynamic connection foundation and confined equipment caused preparing capacities. The peculiar characteristics of the MANET-like open medium, high dynamic nature of the networks leads to enormous attacks, which divides or destroy the entire network. A BH attack is a one, which is employed in opposition to route in MANETS. It is a malicious node which sends the fake reply for RREQ and drops/loss the packets. A malicious node/fake node drop all the traffic in the network, which makes use of the weaknesses of the route/path discovery packets of the on-demand protocols, such as AODV [4]. In the route/path discovery process of AODV protocol, intermediate/mid-way nodes are accountable for detection of a new path to the destination, sending discovery packet BS to the nearby nodes [5].

There are several methods for detection of a BH in MANETs and security is the main concern for safe and efficient communication of packets in mobile nodes. There are many methods like an initially adaptive system of the fuzzy interface to discover and avoid the BH attack. The fuzzy logic deals with such applications more accurately because of its resemblance to human decision making, that is, its ability to produce an exact solution from incomplete or fairly inaccurate information [6]. In order to sense and stop selective BH attacks, the Intrusion detection system (IDS) nodes are organised in MANETs. Anti-BH Mechanism (ABM) function in IDS are exploited to estimate a suspicious value of a node permitting to the abnormal difference among the routing messages transmitted from the node in IDS [7]. ACO is a foraging behavior of swarm of ants may be used to solve complex computational optimization problems. A Routing Protocol (RP) is extremely efficient, adaptive and scalable. The decrease of routing overhead in network is important aim in the design [8]. The well-organized routing mechanism using ACO based Routing Algorithm (ANTALG) is used for better QoS parameters in transmitting networks [9].

Bulletproof verification (BPV) method is one, which pins down the BH node by considering the two steps of the BH detection with the cryptographic mechanism. It does not use flooding to identify the BH node but it is not isolated the BH node from the network [10].

The existing methods have some restrictions such as routing overhead, throughput, energy and security issues. To solve these, highly secured ACO-Dual RSA-BD methodology has been optimized for detecting BH and analysing shortest path in the wireless network. In this work, two essential things like optimization algorithm is used for the purpose of solving the routing problem and find the best direction/path for mobile nodes to reach the destination. Next dual RSA algorithm is utilized for the purpose of mobile nodes security and it communicated with other nodes, for the secure communication. Thus, “ACO-DRSA-BD” gives better results in Throughput, Routing Overhead and energy than the AODV methodology.

The rest of this paper is organized as follows: Section 2, reports on related work. Section 3, presents a review on “ACO-DRSA-BD” Methodology in MANET. Section 4, demonstrated the simulation parameters of the “ACO-DRSA-BD” and Section 5 indicates the conclusion of “ACO-DRSA-BD” research work.

2. Related work

K. Geetha, P. Thangaraj, C.R. Priya, C. Rajan, and S. Geetha [11] has presented Bio-Inspired Integrated Bacterial Foraging Optimization algorithm (IBFO) and Particle Swarm Optimization (PSO) algorithm in MANET routing. The IBFO-PSO techniques are highly adaptive, efficient and scalable. Further work can be improved by using Beehive algorithm (Variant of ACO).

G. Singh, N. Kumar, and A.K. Verma [12] has presented an Innovative ANTALG by considering an irregular assortment of source and destination nodes and exchanges the Ants (agents) between them. Here this algorithm performance parameter was associated with the AODV, ADSR, and HOPNET, conclude that the proposed algorithm gives better throughput and reduced average end to end delay, packet drop, average jitter but security features were not discussed.

V.G. Jebaseelan, and A. Srinivasan [13] has proposed a lightweight curved rectangle vector based secure routing for MANETs. The routing attack targets are identified and avoided by deploying intellectual watchdog and light weighted key verification mechanisms. The packet delivery ratio in the network can be determined in the future.

P.S. Hiremath, T. Anuradha, and P. Pattan [14] has presented adaptive fuzzy interference system for detection and prevention of cooperative blackhole attack in MANETs. Adaptive Fuzzy interference system to prevent and detect the supportive black hole attack on MANETs. The adaptive method increases through-put, end-to-end delay and packet delivery ratio. The adaptive fuzzy logic system shows better performance compared to normal adaptive method. Security is not addressed for efficient transmission of datas.

S. Banerjee, A. Majumdar, H.N. Saha, and R. Dey [15] has demonstrated the Modified ant colony optimization based on routing protocol for MANETs. In multi-hop ad-hoc networks, a new on-demand power balanced routing algorithm for mobile nodes were presented. A Routing Protocol (RP) is extremely efficient, adaptive and scalable.

3. ACO-DRSA-BD methodology

The ACO-DRSA-BD will identify the BH attack in the MANETS and provide a solution with the ACO algorithm for optimum routing. The security is the major concern in any kind of wireless networks; to provide the security we have proposed Dual RSA. The Dual RSA provides less computational time and requires less storage. The key length should be 1024 bits to achieve good security within two minutes. If the key length is less than 1024 bits, it takes within 2 minutes. In Dual RSA two illustrations of RSA will share the same public and private key exponents. So it diminishes the memory requirements for storing both key. Dual RSA is also used to diminish storage requirements. The two different RSA occurrences such as T1=r1s1 and T2=r2s2. The public key (e) and private key (d) should gratify the following equations ed≡1 mod Ø (T1) and ed≡1 mod Ø (T2). Routing for

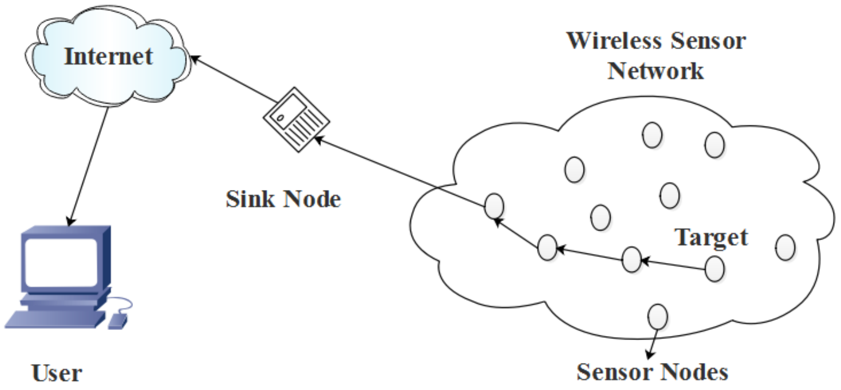
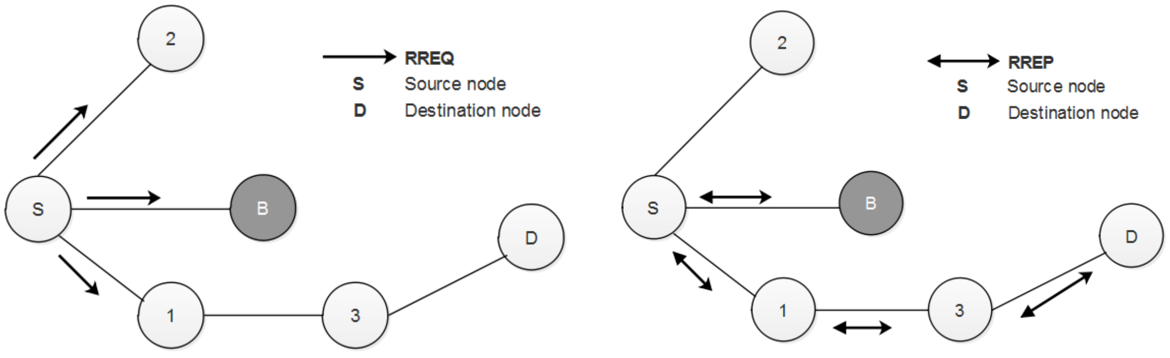


Figure.1 Basic wireless sensor communication



(a) (b)

Figure.2 Occurrence of malicious node B: (a) RREQ and (b) RREP

MANET is a Dynamic Optimization Problem as the search space changes with the time. The routing policy has defined the rule, which specifies what node has to communicate with next node, which is on the way to reach the destination node. The basic diagram of WSN communication is given below in Fig.1. The source node and destination nodes are assigned. The packets are transmitted wirelessly by using intermediate nodes. The sink node acts as the source node, which transmit packets to destination node.

3.1 BH attack Identification/ Malicious Detection

The BH/false node pay attentions to all routing RREQ with the supreme sequence number and less hop count values to the source node, which has a fresh route to the destination. The source node transmits data packets to the destination over false/malicious node. The BH node divert most of the traffic of the network to itself and loss the packets. BH is difficult particularly, if the malicious node uses sequence numbers related to the ones used in the sensor networks. The BH acts very much on the network performance, which make network to behave like false system. If Continuous increase in routing overhead decreases the node's lifetime and lastly leads to network destruction. The RREQ and RREP in occurrence of malicious node is done between sources to destination nodes, which is given in Fig.2.

3.2 Route optimization using ACO algorithm

ACO routing algorithm take attraction from the characteristics of ants in nature and from the related field of ACO to resolve the problems of routing in sensor networks. The main source of motivation is found in the capacity of certain kinds of ants to search the shortest path among their nest and a food sources using Pheromone (Impulsive Chemical Substance). Ant leave traces of pheromone as they migrate between sources to destination. Ants specially go in the course of high pheromone intensities in search of food. The higher levels of pheromone are received, when minimum paths are finished faster. The positive strengthening process allows the colony as a whole to touch on the shortest path.

The probability for ant l at node k moving to node l at generation u is defined as

Key Generation			
Select p, q	p, q *both are prime* $p \neq q$		
Calculate $n = pxq$			
Calculate $\emptyset(n) = (p-1)x(q-1)$			
Select integer e	$\gcd(\emptyset(n), e) = 1; 1 < e < \emptyset(n)$		
Calculate d			
Public key	$KU = \{e, n\}$		
Private key	$KR = \{d, n\}$		
Encryption		**Decryption**	
Plain text	$M < n$	Cipher text	C
Cipher text	$C = M^e(mod\ n)$	Plain text	$M = C^d(mod\ n)$

$$Q_{j,l}^{K}(u) = \frac{t_{j,k}(u)d_{j,k}^{-\beta}}{\sum_{u\in\Gamma^k} t_{j,v}d_{j,v}^{-\beta}}, k \in \Gamma_j^k \quad (1)$$

Where $t_{j,k}$ is the intensity of the pheromone on edges $d_{j,k}$ the distance between nodes i and k, $\Gamma_u^k$the set of nodes that endure to be visited by ant k position at node I to make the solution feasible and$\beta > 0$.

Once all the ants have built their tours, the pheromone is updated on all edges $j \rightarrow k$ according to a global pheromone updating rule.

$$t_{j.k}(t+1) = (1-\rho)_{j,k}\ (t) + \Delta t_{j,k}\ (t) \quad (2)$$

Where

$$\Delta t_{j,k}(t) = \sum_{K=1}^{NP} \Delta\, t_{j,k}^{k}(t) \quad (3)$$

$$\Delta t_{j,k}\ (t) = \begin{Bmatrix} \frac{Q}{Lk}\ , if\ (j,k) \in tour\ done\ by\ ant\ k \\ 0\ ,\ \ Otherwise \end{Bmatrix} \quad (4)$$

$(1-\rho)$ is the pheromone decay parameter $(0 < \rho < 1)$ where it represents the trail evaporation when the ant chosen a city and decide to move Lk is the length of the tour accomplished by ant k and m is the no. of ants.

3.3 RSA and Dual RSA

RSA is an algorithm used by recent computers to encrypt and decrypt data. The Dual RSA is an asymmetric cryptographic algorithm, which have two various keys. The RSA has three algorithms as encryption, decryption and key generation.

3.3.1 RSA Algorithm

RSA cryptography is the popular cryptography system, which is used for security purpose in the wide range of networks. The security border should be raised in the RSA. The most difficult part of RSA cryptography is public and private key-generation. The Prime numbers p and q are created by employing the RSA cryptography. The modulus ‘n’ is subtracted by duplicating P and Q. The no. is exploited by both the general population such as private and public keys between the operators. The one user at the end, sends plain text to the encrypted public key.

3.3.2 Dual RSA

The Dual RSA is basically two distinct instances of RSA that shares the same public and private exponents. To obtain the one Dual RSA, Combining the two instances of the RSA with public key (e, N1 ,N2) and private key(d,p1,q1,p2,q2), where e and d satisfy $ed \equiv 1mod(\phi\ (N_2))$ and $ed \equiv 1mod(\phi\ (N_2))$

From these two relations, it obeys that there exists two positive integer k1 and k2 such that

$$\begin{aligned} ed\ &\equiv 1 + k_1\, \phi\ (N_1) \\ ed\ &\equiv 1 + k_2\, \phi\ (N_2) \end{aligned} \quad (5)$$

The Eq. (5) is called the Dual RSA key equations.

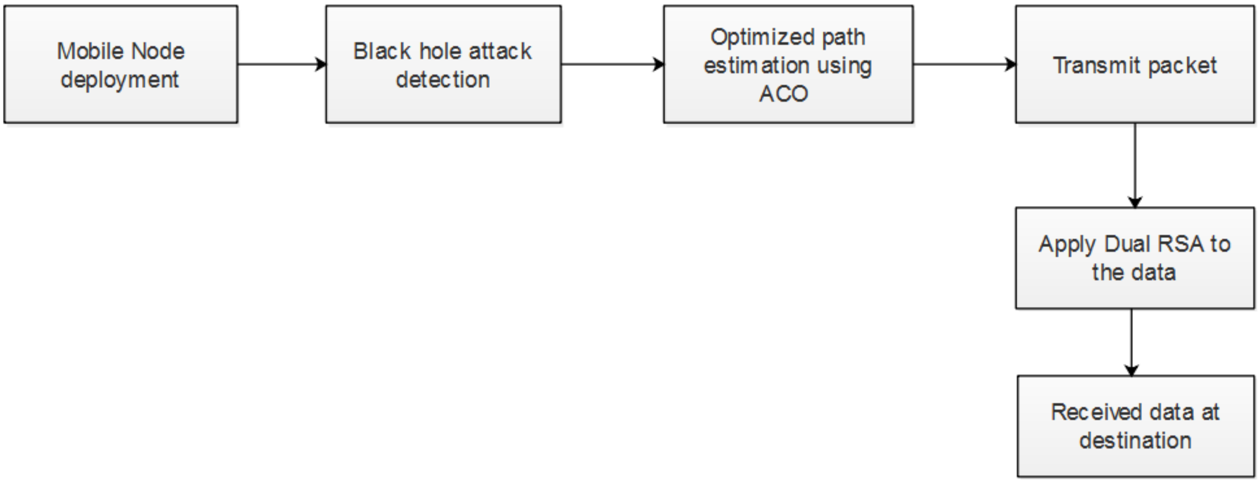

Mobile Node deployment
Black hole attack detection
Optimized path estimation using ACO
Transmit packet
Apply Dual RSA to the data
Received data at destination

Figure.3 Block diagram of efficient detection of BH attack and secured routing using ACO and Dual-RSA

The main idea of key generation algorithms that we contemporary for dual RSA comes from the equation $k_1\, \phi\, (N_1) = k_2\, \phi\, (N_2)$.it sprightly follows from the key (5).the scheme is to build three integers k1, k2, and k3 such that $k2k3\ = (p1 - 1)(q1 - 1)$ and $k1k3 = (p2 - 1)(q2 - 1)$, where $p1, q1, p2$ and $q2$ are all primes.

The Fig.3 shows the block diagram of the BH identification and secured routing using ACO algorithm. Initially mobile nodes are deployed randomly in the interested area, to establish the communication among source and destination node.

The Fig.4 shows the flow chart for BH identification and ACO based routing algorithm. Here finite number of mobile nodes is positioned in the identified area and initially source and destination are assigned in the network. Once source and destination are defined then source node broadcast a RREQ to all the neighbour nodes. If any BH node exists in the network then it responds to source's request with Route Reply Packet (RREP), by obtaining that packet, the source will put the responding node to its black list. Once it is put in to the black list, then awareness based learning become functional for confirmation of the malicious node. If the node is confirmed being malicious then blacklist is updated. The source node informs to all the nodes, if there is any presence of malicious node in the network. Once the malicious node is isolated, optimized path is obtained by using ACO algorithm. If node is not confirmed as a malicious after applying knowledge based learning, then source node has to send fake RREQ packet. With the ACO algorithm optimized path is obtained, then this path is used for communication between source and destination.

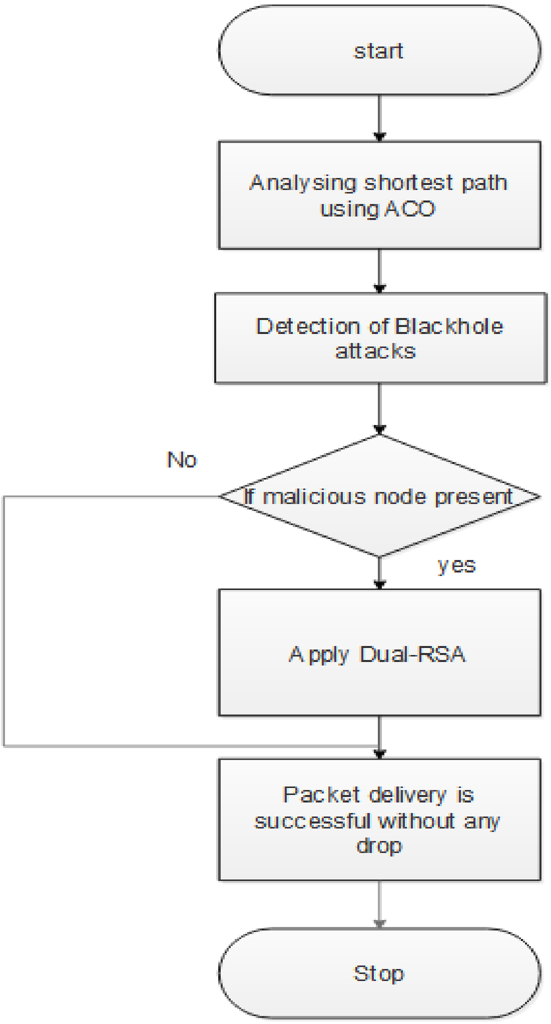

start
Analysing shortest path using ACO
Detection of Blackhole attacks
No
If malicious node present
yes
Apply Dual-RSA
Packet delivery is successful without any drop
Stop

Figure.4 Flow chart of overall Routing process

Received: January 6, 2018

4. Result and discussion

The ACO-DRSA-BD was implemented in NS2 to achieve BH detection and obtain the optimized path for data transmission using ACO algorithm. The complete work was done by using the I7 system with 8 GB RAM. The ACO algorithm was used to obtain the optimized path and Dual RSA for secure transmission through the wireless mobile nodes.

This section gives a detailed view of the results that are obtained using ACO and dual RSA algorithm. ACO-DRSA-BD have proposed Dual RSA algorithm for providing security to the messages contained in the nodes. The experimental results and the performance of through put, routing overhead and energy are compared with the AODV Method.

Comparison analysis of our proposed work is evaluated by varying the nodes 5, 10, 15, 20, 25, 30. Figs. 4, 5 and 6 show the comparison of throughput, routing overhead and energy between proposed and the AODV methods.

Throughput and energy consumption is increased with a decrease in routing overhead. The Performance metrics is given below;

4.1 Throughput

Throughput is calculated based on total packets received at the destination node by total network time.

$$\text{Throughput} = \frac{\text{Total packets received at the destination node}}{\text{Tota l simulation time}}$$

4.2 Routing overhead

Routing Overhead is the quantity of routing packets requires for network communication, which is divided by a total number of distributed data packets.

RH = Total no. of routing packets/Total no. of delivered data packets.

4.3 Energy consumption

The huge number of hops is equivalent to the huge amount of received energy consumption. A node drops a specific amount of energy for every packet transmission and received.

Number of mobile nodes are deployed based on 5, 10, 15, 20, 25 and 30 by measuring different parameters such as Through-put, Routing Overhead and Energy Consumption with AODV and ACO-DRSA-BD Methodology, which is given in Table 1.

Table 1. Comparison between ACO-DRSA-BD method and AODV method

Number of Mobile Nodes	Throughput		Routing Overhead		Energy Consumption	
	AODV	ACO-DRSA-BD	AODV	ACO-DRSA-BD	AODV	ACO-DRSA-BD
5	939	943	100	80	4.2	4.2
10	942	950	150	100	5.0	5.0
15	953	960	155	147	5.5	5.9
20	969	975	175	150	5.6	5.9
25	970	980	185	165	5.9	6.0
30	973	983	183	165	5.8	6.0

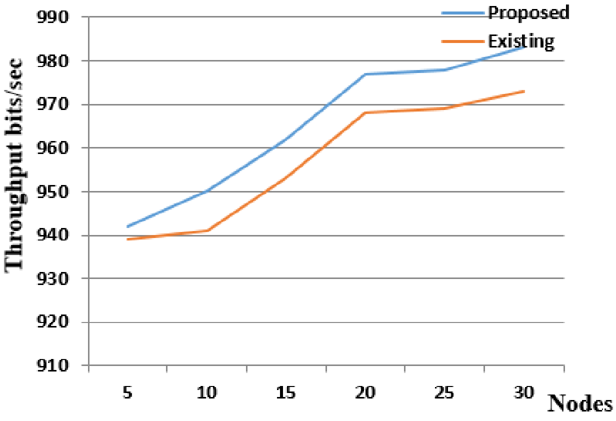


Figure.5 Nodes vs. Throughput

Received: January 6, 2018

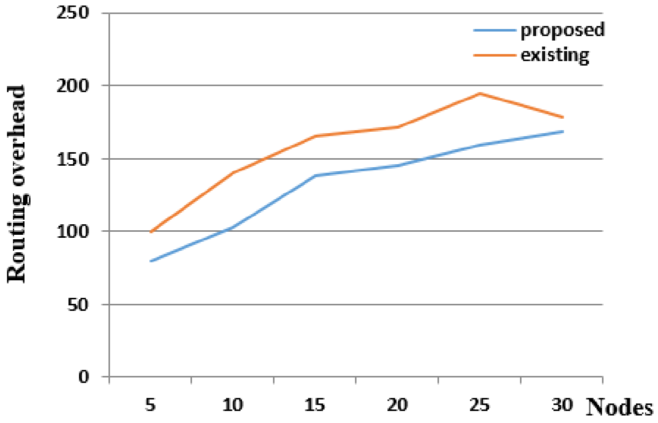


Figure.6 Nodes vs routing Overhead

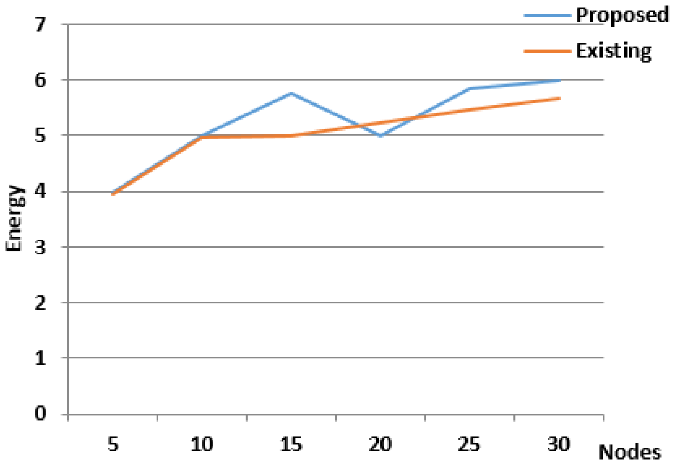


Figure.7 Nodes vs. Energy

The Comparison of Nodes vs throughput between proposed and AODV is plotted in Fig.5. The Throughput value is increased in ACO-DRSA-BD method compared to the AODV methods. Throughput for 5, 10, 15, 20, 25 and 30 nodes is 950, 960, 975, 980 and 983 bits/sec respectively for ACO-DRSA-BD Method.

The comparison of Nodes vs routing Overhead between proposed and AODV method is plotted in Fig.6. The routing overhead comparison of the ACO-DRSA-BD and AODV method is depicted with respect to the different nodes. Routing Overhead for 5, 10, 15, 20, 25 and 30 nodes are 80, 100, 147, 150, 165 and 165 respectively for ACO-DRSA-BD Method.

The comparison of Nodes vs Energy between proposed and AODV method is plotted in Fig.6. The energy value of ACO-DRSA-BD method is increased compared to the AODV methods. Energy Consumption for 5, 10, 15, 20, 25 and 30 nodes is 4.2, 5.0, 5.9, 5.9, 6.0 and 6.0 respectively for ACO-DRSA-BD.

The Nodes deployment in NAM Animator Window is shown in following Figs. 8, 9, 10, 11, and 12. The Screenshots of NAM Animator window is shown below.

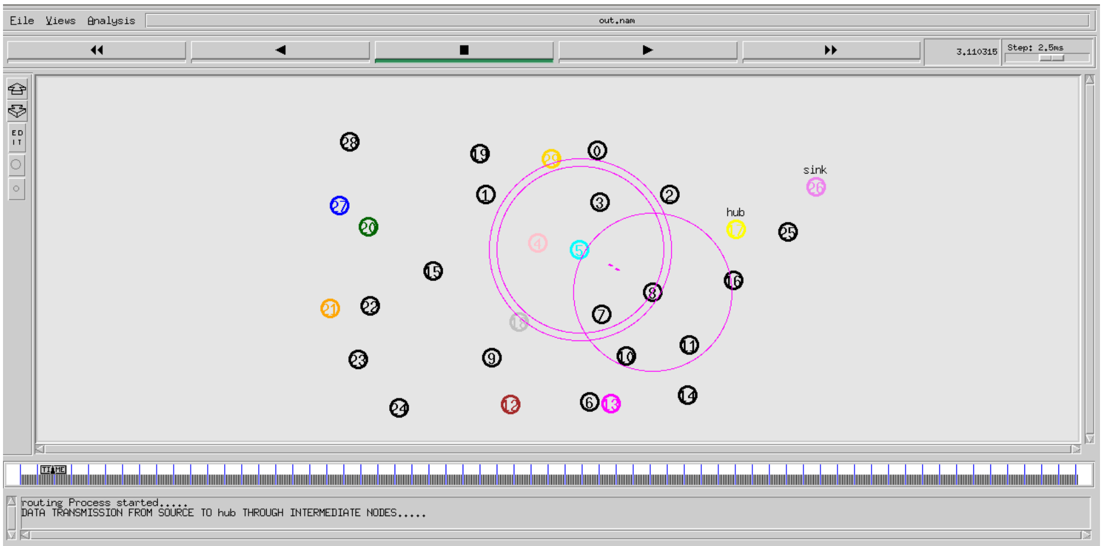
The Pink round indicates the routing refresh process of each and every node. Routing process from source to destination takes place.

In Fig.9 the routing process are started by analysing the shortest path in the network using ACO. The shortest path analysis is done using optimization techniques. Packet transmission takes nodes between each and every nodes.

In Fig.10, the malicious nodes send request to the source nodes giving acknowledgment that it is the destination node. The packets are dropped/loss due to the malicious happenings in the various nodes. A node broadcast RREQ from source to destination by monitoring data flow. Due to the malicious nodes activity the packets dropped.

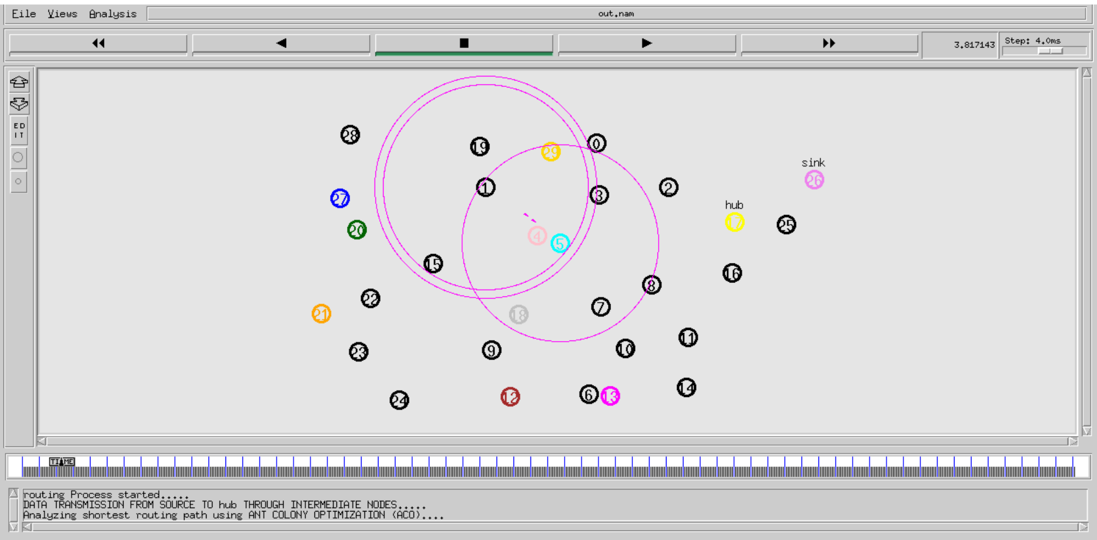
The Detection of BH attack in the different nodes is analysed in the Fig.11. The packets are dropped in 1, 2, 3, 19 and 29 nodes. Another shortest path is analysed by choosing secured path through nodes (20-23-9-13-11-17), which doesn't have malicious nodes/false nodes in this path.

Received: January 6, 2018



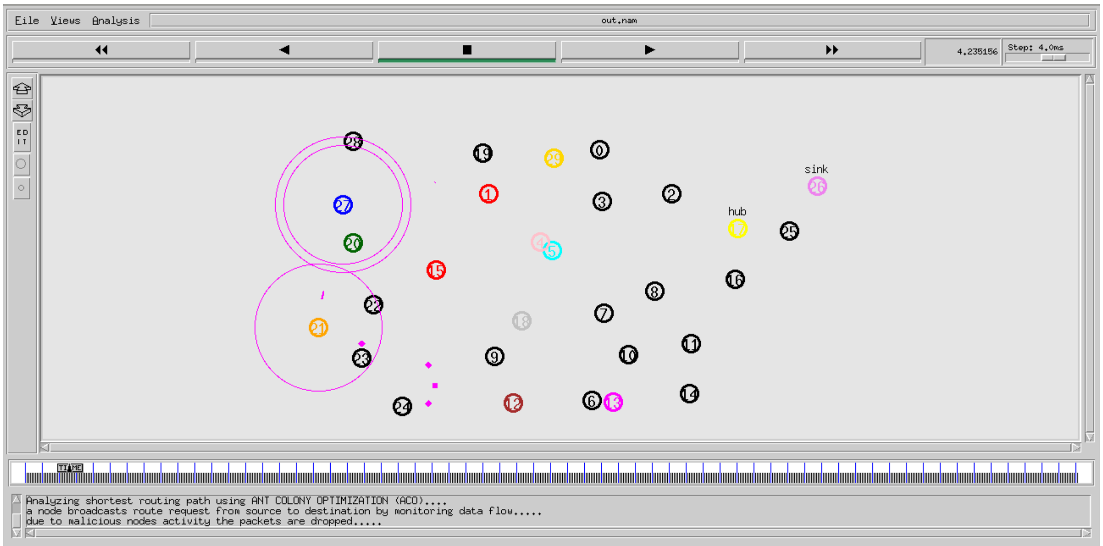
```
routing Process started.....
DATA TRANSMISSION FROM SOURCE TO hub THROUGH INTERMEDIATE NODES.....
```

Figure.8 Data transmission from source through intermediate nodes



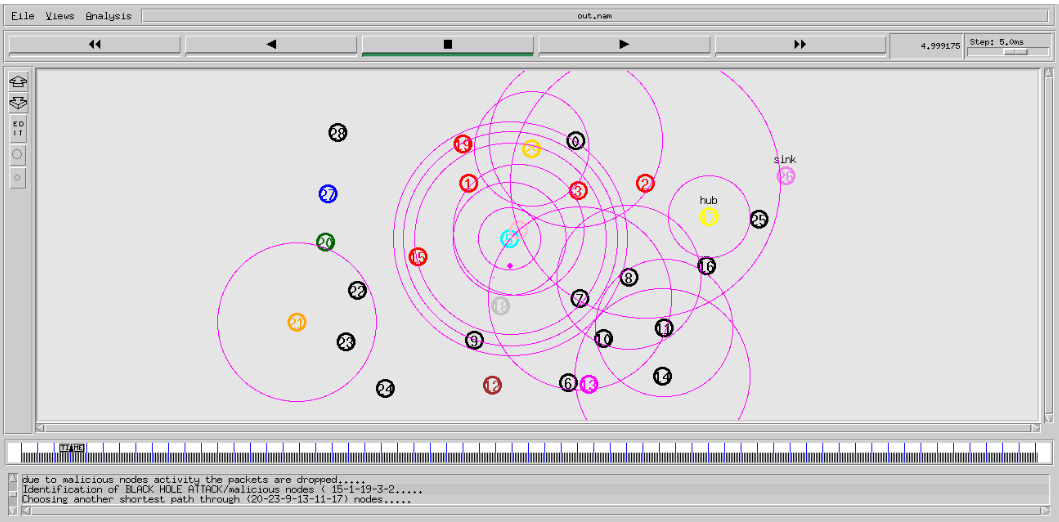
```
routing Process started.....
DATA TRANSMISSION FROM SOURCE TO hub THROUGH INTERMEDIATE NODES.....
Analyzing shortest routing path using ANT COLONY OPTIMIZATION (ACO)....
```

Figure.9 Data transmission from source to destination by analysing shortest path in the network



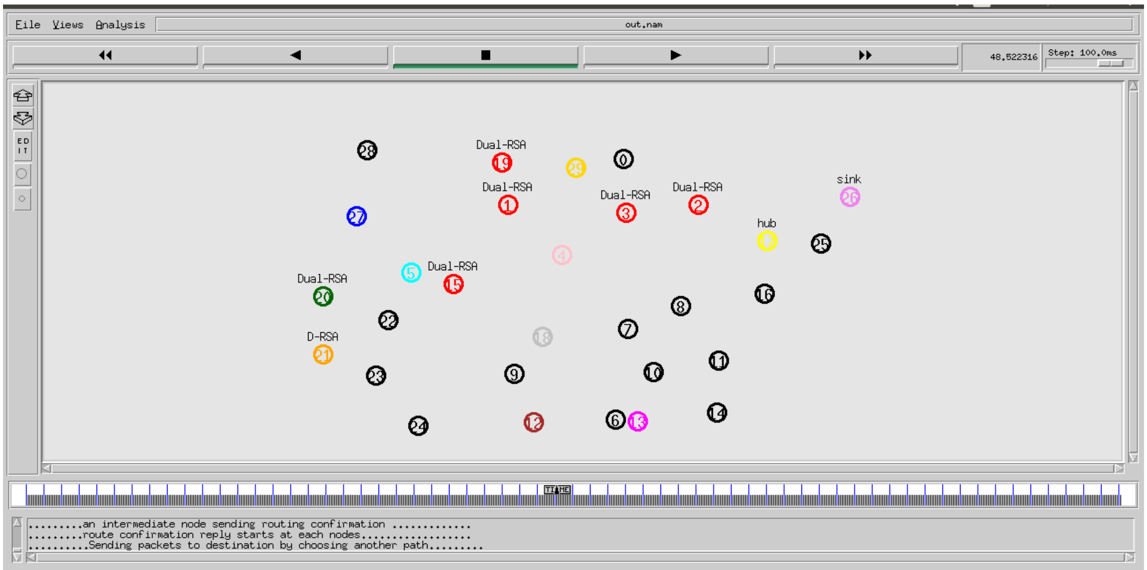
```
Analyzing shortest routing path using ANT COLONY OPTIMIZATION (ACO)....
a node broadcasts route request from source to destination by monitoring data flow.....
due to malicious nodes activity the packets are dropped.....
```

Fig.10 Packets dropped due to malicious node activity in the network



```
due to malicious nodes activity the packets are dropped.....
Identification of BLACK HOLE ATTACK/malicious nodes ( 15-1-19-3-2.....
Choosing another shortest path through (20-23-9-13-11-17) nodes.....
```

Figure.11 Detection of BH attack



```
.........an intermediate node sending routing confirmation .............
.........route confirmation reply starts at each nodes..................
..........Sending packets to destination by choosing another path.........
```

Figure.12 Using Dual-RSA for security

Fig.12 shows that the Dual-RSA key management techniques are applied in the nodes for security purpose in the network. Hence, shortest path is analysed using ACO algorithm. Finally, all packets are successfully transmitted from source to destination without any loss of packets. Dual-RSA encryption and decryption is applied to the nodes for maintaining secured transmission of data in the sensor networks.

The ACO-DRSA-BD has precisely detected the BH node and discover the solution for data transmission using ACO algorithm in secured environment. Thus the ACO-DRSA-BD gives improved results in through put, routing overhead and energy associated with the AODV method. Table 2 denotes simulation parameters used in ACO-DRSA-BD methodology.

Table 2. Simulation parameters

Routing algorithm	ACO
Security algorithm	Dual RSA
Simulator used	NS2
Packets Send	2087
Packets Received	2067
Dropped packets	20
Simulation start time	1.000000000
Simulation End time	4.999938867
Number of mobile nodes	30
Antenna Model	Omni Antenna
Minimum speed	2.0 ms
Network Interface types	Wireless

5. Conclusion

ACO-DRSA-BD Methodology is used for detection of the BH in the network and by isolating the optimized path and shortest path using ACO algorithm. The ACO-DRSA-BD methodology has achieved the best path selection and secure data transmission over the mobile nodes in wireless environment. The essential ACO algorithm is used for the purpose of solving the routing problem and find the best route for transmitting data packets to reach the destination. Dual-RSA is used for encryption and decryption of data, if there is any black-hole or Malicious node in the networks. From obtained results, we concluded that the ACO-DRSA-BD method has reached the best routing and better Throughput, Routing overhead and Energy compared to the AODV algorithms by deploying various nodes. Hence, throughput in ACO-DRSA-BD is 10% increased than AODV method. Routing overhead in ACO-DRSA-BD is 22% decreased than AODV method. Energy consumption is 5% decreased than the AODV Method.

As a Future Scope, hybrid cryptography or Advanced Encryption Standard (AES) can be used for improving security in the ad-hoc network.

References

[1] R. Ranjan, N.K. Singh, and A. Singh, “Security issues of BH attacks in MANET”, In: *Proc. of International Conf. on Computing, Communication & Automation (ICCCA),* 2015.

[2] A. Sardana, T. Bedwal, A. Saini, and R. Tayal, “BH attack's effect mobile ad-hoc networks (MANET)”, In: *Proc. of International Conf. On Computer Engineering and Applications (ICACEA)*, pp. 966-970, 2015.

[3] G. Singh, N. Kumar, and A.K. Verma, “OANTALG: An orientation based ant colony algorithm for mobile Ad Hoc networks”, *Wireless Personal Communications,* Vol.77, No.3, pp.1859-1884, 2014.

[4] N. Jaisankar, R. Saravanan, and K.D. Swamy, “A novel security approach for detecting BH attack in MANET”, *Information Processing and Management*, pp.217-223, 2010.

[5] R. Das, B.S. Purkayastha, and P. Das, “Security measures for BH attack in manet: An approach”, arXiv preprint arXiv:, Vol.1206, No.3764, 2012.

[6] P.S. Hiremath, T. Anuradha, and P. Pattan, “Adaptive fuzzy inference system for detection and prevention of cooperative BH attack in MANETs”, In: *Proc. of International Conf. on* Information Science (ICIS), pp.245-251, 2016.

[7] M.Y. Su, “Prevention of selective BH attacks on mobile ad hoc networks through intrusion detection systems”, *Computer Communications*, Vol.34, No.1, pp.107-117, 2011.

[8] S. Sharma, M. Singh, and G. Singh, “Realistic inspection of proposed Ant algorithm with Antnet algorithm using NS-2”, *International Journal of Research in IT, Management and Engineering*, Vol.2, No.6, pp.146-156, 2012.

[9] G. Singh, N. Kumar, and A.K. Verma, “Antalg: An innovative aco based routing algorithm for manets”, *Journal of Network and Computer Applications*, Vol.45 pp.151-167, 2014.

[10] F. Ahmed, S. Yoon, and H. Oh, “Bullet-proof verification (BPV) method to detect BH attack in mobile ad hoc networks”, In: *Proc. of International Conf. on Ubiquitous Intelligence and Computing*, pp.435-449, 2011.

[11] K. Geetha, P. Thangaraj, C.R. Priya, C. Rajan, and S. Geetha, “IBFO_PSO: Evaluating the Performance of Bio-Inspired Integrated Bacterial Foraging Optimization Algorithm and Particle Swarm Optimization Algorithm in MANET Routing”, *World Academy of Science, Engineering and Technology, International Journal of Mathematical, Computational, Physical, Electrical and Computer Engineering*, Vol.9, No.3, pp.194-200, 2015.

[12] G. Singh, N. Kumar, and A.K. Verma, “Antalg: An innovative aco based routing algorithm for manets”, *Journal of Network and Computer Applications*, Vol.45, pp.151-167, 2014.

[13] V.G. Jebaseelan and A. Srinivasan, “ArcRectZone: A Lightweight Curved Rectangle Vector Based Secure Routing for Mobile Ad-Hoc Sensor Network”, *International Journal of Intelligent Engineering and Systems,* Vol.10, No.6, pp.116-124, 2017.

[14] P.S. Hiremath, T. Anuradha, and P. Pattan, “Adaptive fuzzy inference system for detection and prevention of cooperative black hole attack in MANETs”, In: *Proc. of International Conf. On Information Science (ICIS),* pp.245-251, 2016.

[15] S. Banerjee, A. Majumdar, H.N. Saha, and R. Dey, “Modified Ant Colony Optimization (ACO) based routing protocol for MANET”, In: *Proc. of International Conf. On Computing and Communication (IEMCON),* pp. 1-7, 2015.