FUDMA Journal of Sciences (FJS)
ISSN: 2616-1370
Vol. 2 No. 1, April, 2018, pp 187-193

AN ENHANCE APPROACH FOR DETECTING AND PREVENTING SINGLE AND COLLABORATIVE ATTACKS IN MOBILE AD-HOC NETWORKS

Abdulrashid Sabo[1], A Lawan[2]

[1]*(Department of Computer Science, Bayero University Kano, Nigeria)*
[2]*(Department of Information Technology, Bayero University Kano, Nigeria)*
*Corresponding authors email: dean.csit@buk.edu.ng

ABSTRACT

Mobile ad hoc network is a system of wireless mobile nodes that are dynamically self-organize in arbitrary and temporary topologies, with no fixed set of communication infrastructure and lack centralized administration, where network devices are inter-connected through wireless interface. Mobile nodes in Mobile ad-hoc Networks not only act as a host but as a router or relay stations for forwarding packets from source to destination. The dynamic nature and other characteristics of MANETs such as nodes mobility dynamic and topological changes makes it highly susceptible to various security attacks ranging from collaborative black hole/ gray hole attacks, sink hole attacks to eavesdropping attacks. The mentioned attacks mainly disrupt the routing process by giving false routing information in MANETs, thus finding safe routing path by avoiding malicious nodes is a genuine challenge. The research work aim at in cooperating RSA encryption algorithm to the cooperative bait detection scheme. The proposed work allow the source to use public key crypto system (in this case RSA) to encrypt data before transmitting it to the destination after the initial reverse tracing operations, it eliminate the used threshold value to indicate the reoccurrence of malicious nodes, it also eliminate the use of confirmation RREQ, since the public key cryptosystem introduced by the proposed work is sufficient enough to cover the transmitted data from an unknown attacker. The research work was simulated using network simulator tool NS2 and simulation results shows that the proposed works show an increase in packet delivery ratio, and a remarkable decrease in routing overhead.

Keywords-*MANET, CBDS, Black hole, RSA and eavesdropping*

INTRODUCTION

Past few years have witnessed rapid growth in the area of mobile computing due to proliferation of widely available inexpensive wireless devices; this has opened opportunity for researchers to work on wireless mobile ad hoc networks, MANETs (Chang, et al., 2014). MANETs is a system of wireless mobile nodes that are dynamically self-organized in arbitrary and temporary topologies (Boora & Ohri, 2013) which has no fixed set of communication infrastructure and lack centralized administration. The network devices in MANETs are interconnected through wireless interface, thus mobile nodes not only act as a host but as routers or relay station for forwarding data from source to destination. Due to its characteristics MANETs have been used for various important applications such as emergency preparedness and response operations and military crisis operation.

A lot of research works concentrated on the security of MANETs, most of which deal with the prevention and detection approaches to combat individual and collaborative misbehaving nodes, with no well-known message security scheme to prevent unauthorized reading and writing of the transmitted data. In this regard the effectiveness of these approaches become weak when an unauthorized nodes can easily read or write the transmitted data or can be able to take confidential information that should be kept secret and may lead to a more devastating damage to the networks.

The dynamic nature and other characteristics of MANETs such as lack of communication infrastructure, dynamic change in topologies, node mobility and lack of centralized administration make it highly susceptible to various security attacks, such as cooperative black hole (a black hole is an active internal attack where a malicious node falsely replies for any route request RREQ message without having active route to the specified destination and drop all receiving packets (Rana, et al., 2014). A situation where multiple black hole nodes work together to cause serious damage to the network by launching cooperative attack it is called cooperative black hole attack , gray hole(A gray hole attack is an internal attack where the mobile node is not initially malicious, it turns malicious sometime later during the network operations (Suntana & Kazi, 2015) attacks, sinkhole and eavesdropping (another kind of passive attack that aim at obtaining some confidential information that should be secrete during communication) attacks. Though the basic requirement for a secured network are secured routing protocols which ensure the confidentiality, availability, authenticity and integrity of data transmission and these attacks mainly disrupt the routing process by giving false routing information in MANETs. Hence detecting and preventing these attacks to make a secured routing framework in MANETs to prevent it against miscreant is a great challenge.

This paper propose a scheme that prevent and detect the reoccurrence of cooperative black hole/gray hole attacks by incorporating a well-known message security scheme in this case RSA public key cryptosystem to the existing cooperative bait detection scheme (CBDS) (Chang, et al., 2014), in order to construct a comprehensive secure routing framework to protect MANETs against miscreant. The proposed scheme was simulated using network simulation tool NS2 and simulation results shows that the proposed scheme out performs the existing CBDS in terms of packet delivery ratio and routing overhead.

Dynamic source routing (DSR), which is among the features of the existing system that the proposed scheme maintained, it is a uni-path routing protocol specifically designed for use in multi-hop networks consisting of mobile nodes (Mustpha, et al., 2016). This protocol mainly involved two main processes which are route discovery and route maintenance processes. The route discovery process is first executed whenever a node needs to send data to another node if it doesn't already have route to the intending destination in its route cache by broadcasting a route request packet RREQ a feature that the malicious nodes uses to send fake route replies. The route maintenance process allows the source nodes to maintain connection even if there is link breakage by generating a route error packet that will update the source node about the link failure and if there is a node that has an alternative path, then the data will be routed through it. Otherwise source node has to invoke the route discovery process again. DSR invoke both route discovery and route maintenance processes on-demand.

RELATED WORK

.An algorithm that prevents the cooperative black hole attacks in mobile ad hoc networks was presented. The algorithm is based on a trust relationship between nodes and hence it cannot tackle gray hole attacks. Besides due to intensive cross-checking, the algorithm takes more time to complete, even if the network is not under attack (Ramaswamy, et al., 2013).

A mechanism that used a unique protocol for identifying and removal of cooperative black hole and gray nodes in mobile ad hoc networks, with the help of a backbone network of trusted nodes for restricted IP (RIP) addresses was proposed (K & Paul, 2010). The scheme lacks message security scheme, so it can't tackle eavesdropping attacks.

A mechanism named cooperative bait detection scheme CBDS based on DSR routing protocol or detecting and preventing collaborative black hole and gray hole attacks was presented. It allows the source node to use the address of its neighbor as bait destination address to bait malicious node replies with fake routing information and implement a reverse tracing algorithm to detect the malicious nodes (Chang, et al., 2014). The scheme can be enhanced by integrating it with a well-known message security scheme to construct a secured routing frame work to prevent MANETs against malicious nodes.

An approach for detecting collaborative black hole attacks by enhancing the features of ad hoc on-demand routing protocol AODV by adding a secured reliable route request SRR_REQ and a secured reliable route reply SRR_REP with a reliability list RL and a threshold value TV as routing entries to the traditional AODV was presented (Rana, et al., 2014).

A survey on secured cooperative bait detection approach for detecting malicious nodes in MANETs was described (M. & M, 2015). The problem of security with formation of communication among nodes is executed together by the nodes themselves. Thus preventing or sensing malicious nodes launching gray hole / collaborative black hole attack is the main challenge. The CBDA combine both proactive and reactive defense architecture.

A scheme that uses a circular ring of tokens generated to bait selfish and malicious nodes was presented. Once token neighboring nodes are received to simulate bait RREQ to all other nodes with bait tokens, all other nodes including selfish and malicious nodes send to replies corresponding source node. Then backtracking is applied to detect the route path from all the nodes (Mustpha, et al., 2016). It lacks a message security scheme to send data with security.

METHODOLOGY

This paper aim to in cooperate RSA encryption scheme to the CBDS and employ the following methods and procedures in order to detect and prevent collaborative black hole/gray hole attacks in mobile ad hoc networks. It starts by using network simulator NS2 to create mobile wireless nodes scenario and then:

A. Neighbor selection algorithm

This algorithm allows all nodes in the network to know all their neighbors by computing the distances between each node and compare it with the transmission range. If it is less than the transmission range then it will be listed among the neighbors of that node else it will not be listed.

B. Initial Bait Setup

The initial bait setup is used to tempt malicious nodes to send RREPs messages when a bait RREQ message is sent to it. Here the source node randomly chooses the address of one of its neighbor node as bait destination address to tempt malicious node to send a RREP message when a bait RRQ message is sent to it, the malicious node use to advertise itself as having the shortest route to the destination (Ramaswamy, et al., 2013). It then calls the reverse tracing algorithm to trace and recheck the RREPs to detect malicious nodes RREPs.

C. Reverse Tracing Algorithm

The reverse tracing algorithm is utilized to identify the behavior of malicious nodes through the RREP to the bait RREQ message. If a malicious node had receive the bait RREQ, it will then reply with a fake RREP, then the reverse tracing operations will be initiated for the nodes receiving the RREP, with the goal of detecting the dubious information and temporarily trusted nodes (M. & M, 2015). Initially an address list P-List and a route information list K_k-List are created.

$P = \{n1 \dots nk \dots n_m \dots nr\}$ (1)

$K_k = \{n1 \dots nk\}$ (Chang et al., 2014) (2)

Node nkdetermine the difference between the address lists

$$K_k' = P_{List} - K_k\_List$$

$K_k' = \{nk + 1 \dots n_m \dots nr\}$ (PP & Chacko, 2013) (3)

K_k'-list = is now stored in the RREPs and then they are reverted to the source node.

The source node receives the RREP, and the K_k'-list of the nodes which receives the RREP, in order to ensure that the list does not come from a malicious node. After receiving the RREP, node nk recheck the RREP by comparing

1. The source address in the IP fields of the RREP
2. The next hop of nk in the $P = \{n1 \dots nk \dots n_m \dots nr\}$ and
3. One hop of nk

The dubious path information S is computed as shown in equation (4)

$S = K_1' \cap K_1' \cap \dots K_n'$ (Suntana & Kazi, 2015) (4)

The trusted set T is given by

$T = P - S$ (Abinaya & , 2016) (5)

To confirm that the malicious node is in set S, the source node send a test packet to this route and a recheck packet to the second towards the last node in set T. Finally the source node stores the malicious nodes in a black list and then broadcast an alarm packet throughout the network to inform all nodes to terminate their operation with these nodes (Abinaya & , 2016).

D. The RSA encryption algorithm

The public key cryptosystem (RSA) was in cooperated in to the CBDS because of its reliance on a public encryption algorithm, a public decryption algorithm and a public encryption key (Foruuzan, 2008). It also allow the use of public key and an encryption algorithm so that every node in MANETs can encrypt a message and only an authorize node that knows the private key can decrypt data using a decryption algorithm and the private key. The public key cryptosystem (RSA) consist of the following procedures:-

I. RSA key generation process
II. RSA encryption algorithm and
III. RSA decryption algorithm

1) RSA key generation

Any node that wishes to participate in the network should generate a pair of keys, namely public key (n, e) and private key is (n, d).

Select two prime numbers p, q

Compute the RSA modulo n

$$n = pq \qquad (6)$$

Compute $\emptyset(n) = \emptyset(p) * \emptyset(q)$

$$=(p-1)(q-1) \qquad (7)$$

Choose e such that 1<e<$\emptyset(n)$ and gcd ($\emptyset(n)$, e) = 1

Compute d such that d = e^{-1}(mod$\emptyset(n)$)

$$de=1(\mathrm{mod}\,\emptyset(n)) \qquad (8)$$

The public key (n, e) and the private key (n, d)

2) RSA Encryption

The source node obtains the public key (n, e), represents the plaintext message as a positive integers P, and compute the cipher text C and sends it to the destination node.

$C = P^e(mod\ n)$ (Musa, et al., 2015) (9)

3) RSA Decryption

The destination node receives the cipher text C, use its private key to compute the plaintext P

$P = C^d(mod\ n)$ (Musa, et al., 2015) (10)

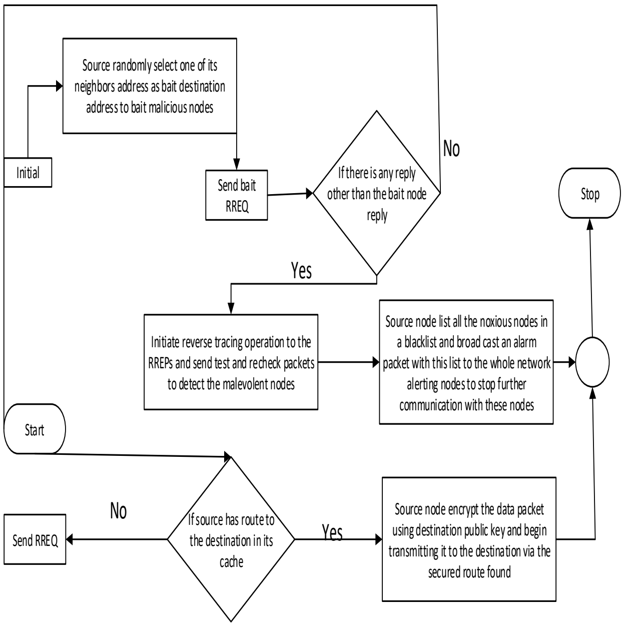
Source randomly select one of its neighbors address as bait destination address to bait malicious nodes
Initial
Send bait RREQ
If there is any reply other than the bait node reply
No
Yes
Stop
Initiate reverse tracing operation to the RREPs and send test and recheck packets to detect the malevolent nodes
Source node list all the noxious nodes in a blacklist and broad cast an alarm packet with this list to the whole network alerting nodes to stop further communication with these nodes
Start
No
Send RREQ
If source has route to the destination in its cache
Yes
Source node encrypt the data packet using destination public key and begin transmitting it to the destination via the secured route found

Figure 1 Basic operation of the proposed work (adapted from (Chang, et al., 2014))

PERFORMANCE EVALUATION

Network simulator tool NS2 is used to study the performance of the proposed enhanced approach for detecting and preventing single and collaborative attacks in MANETs, the paper employ IEEE 802.11 MAC with channel data rate of 11Mbps, Omni-Antenna as the antenna model, TwoRayGround radio propagation model, and a wireless physical interface. All remaining simulation parameters are stated in table 1. The network used for the simulation is captured in fig 1.2; in the simulation malicious nodes are selected randomly to perform attacks in the network.

Table 1: Simulation parameters

Parameters	Values
Number of nodes	50
Area	700m by 700m
MAC	MAC IEEE 802.11
Application traffic	CBR
Radio Range	250m
Channel data Rate	11mbps
Pause time	0s
Maximum speed	20m/s
Malicious nodes	5
Simulation Time	20s

Table 1 simulation parameters adopted in (Chang, et al., 2014)

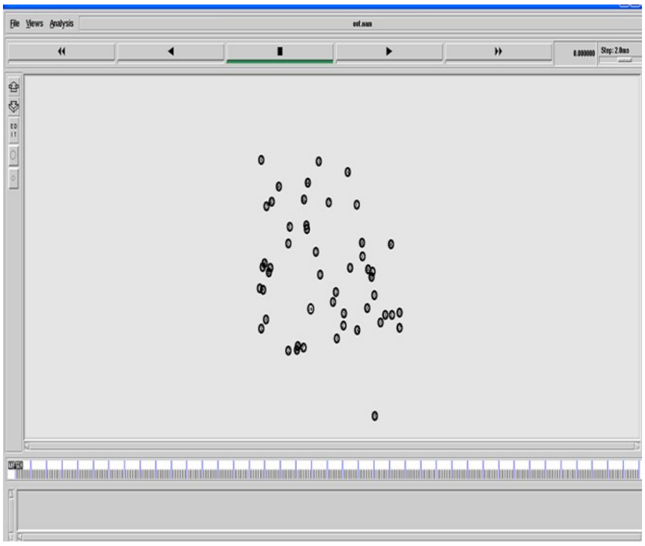

Figure 1.2 Network topology

Performance Metrics

The proposed enhanced approach for detecting and preventing single and collaborative attacks in MANETs is compared to the existing cooperative bait detection scheme proposed in [1] chosen as benchmark on the basis of the following performance metrics.

4) *Packet delivery ratio*

Packet delivery ratio is defined as the ratio of the number of data packets received by the destination to the number of packets sent by the source. Mathematically, it can be defined as:

$PDR = pktd \ \div pkts$ (Adapted from (Chang, et al., 2014)) (11)

Where $pktd$the sum of the data packets is received by the destination and $pkts$ is the sum of the data packets sent by the source node.

5) *Routing overhead*

Routing overhead represent the ratio of the routing related control packets transmission to the amount of data transmissions.

$RO = cpk \ \div pkt$ (Adapted in (Chang et al., 2014)) (12)

Where cpk is the sum of the number of control packets transmitted in the application traffic and pkt is the sum of the number of data packets transmitted in the application traffic and the routing overhead is denoted by RO.

Two simulation scenarios are considered

1) Scenario 1: under fixed mobility and fixed percentage of Malicious nodes
2) Scenario 2: under varying mobility and fixed percentage of malicious nodes

Under these scenarios the performance of the enhance approach for detecting and preventing single and collaborative attacks in MANETs is studied in order to see the effect of the RSA cryptosystem incorporated to the existing cooperative bait detection scheme on the aforementioned performance parameters. The simulation results are shown below.

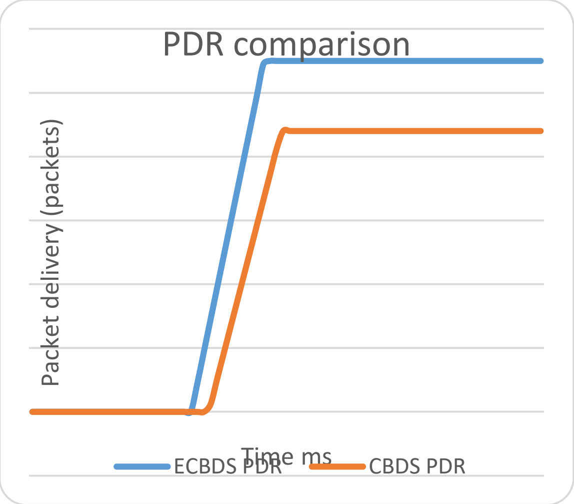

Figure 1.3 PDR comparisons under fixed mobility and percentage of malicious nodes

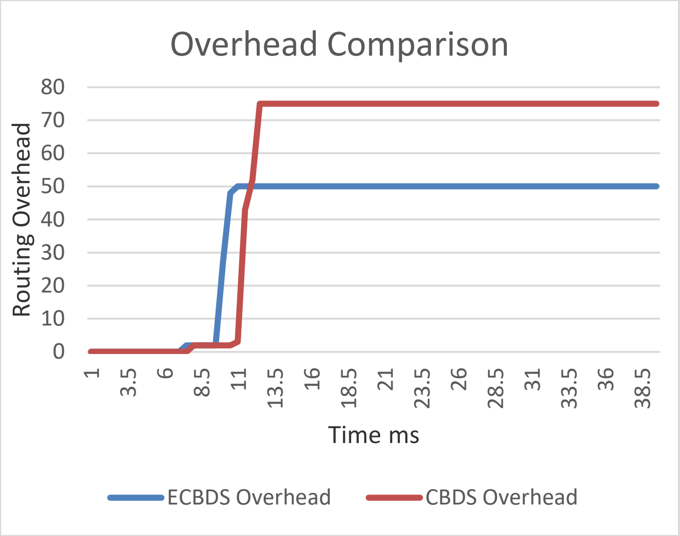

Figure 1.4 Network throughput comparison under fixed mobility and percentage of malicious nodes

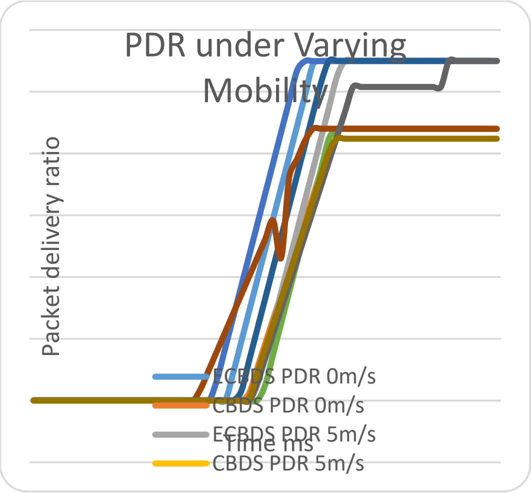

Figure 1.5 Packet delivery ratios under varying mobility

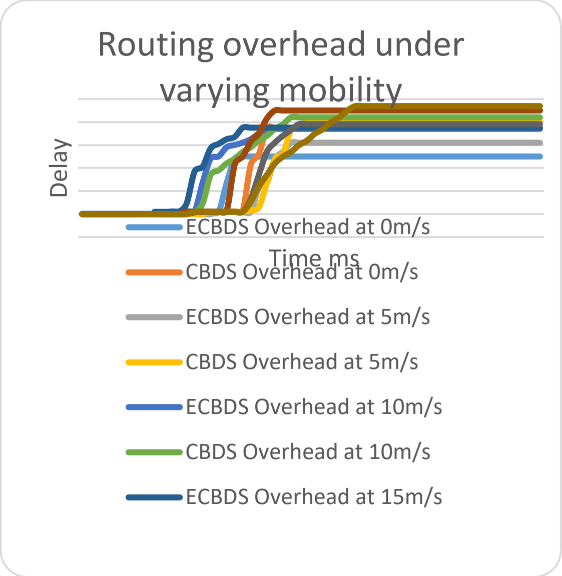

Figure 1.6 routing overhead under varying mobility

RESULTS DISCUSSION

Figure 1.3 compares the packet delivery ratio of the proposed enhanced approach for detecting and preventing single and collaborative attacks in MANETs and that of the cooperative bait detection scheme proposed (Chang, et al., 2014) under fixed percentage of malicious nodes and fixed mobility, it can be observed from the graphs that the proposed work out performs the CBDS in terms of the delivery ratio and this is attributed to the fact that the proposed work uses the RSA cryptosystem to prevent reoccurrence of malicious nodes after the initial reverse tracing operation whereas in the CBDS the reverse tracing operation is only recalled to detect the reoccurrence of malicious nodes only when the delivery ratio is below the threshold value, hence cannot detect malicious nodes when presence in the network after the initial reverse tracing and the delivery ratio is net below the threshold value. Also the proposed work can prevent eavesdropping attacks by using the RSA cryptosystem to prevent the eavesdropping nodes from unauthorized reading of the data content which is not the case in the existing CBDS.

Figure 1.4 shows the routing overhead of the two scheme under fixed mobility and percentage of malicious nodes, from the figure, it can be observed that the existing CBDS produces more overhead compared to the existing enhanced approach for detecting and preventing single and collaborative attacks in MANETs and this is due to the use of more control packets by the CBDS when using the threshold value to recall the reverse tracing operation after its initial used, whereas the proposed scheme eliminate the use of the threshold value used in the CBDS to minimizes the use of control packets which help reduce the overhead.

Figure 1.5 shows the delivery ratio of the proposed scheme and that of the existing CBDS scheme under fixed percentage of malicious node and maximum node mobility speed of 0 to 20m/s. From the figure it can be observed there is a little or negligible decrease in the delivery ratio for both schemes whenever there is increase in node mobility speed. The proposed scheme produces more delivery ratio at 0m/s, 5m/s, 10m/s, 15m/s and 20m/s respectively, than the existing CBDS scheme.

Figure 1.6 shows the routing overhead simulation results of the proposed scheme and that of the existing CBDS under varying node mobility speed, though the routing overhead of the two schemes increases with increase in node mobility speed, the proposed work produces lower overhead than the existing CBDS at all levels and this is because it employ the use of more routing control packets than the existing scheme which help increase the overhead.

CONCLUSION AND FUTURE WORK

This paper present an enhanced approach for detecting and preventing single and collaborative attacks in mobile ad-hoc networks by incorporating an RSA public key cryptosystem to the existing cooperative bait detection scheme for detecting and preventing cooperative black hole/gray hole attacks in mobile ad-hoc networks. Two simulation scenarios were considered in the research work, under fixed mobility and fixed percentage of malicious nodes, and under varying node mobility and fixed percentage of malicious nodes in the network. In these scenarios the performance of the proposed work outperforms the existing CBDS scheme in terms of packet delivery ratio and routing overhead. Simulation result shows that incorporating an RSA public key cryptosystem to the existing CBDS scheme may construct a secured routing frame work that may prevent MANETs against malicious nodes. In future the effect of the proposed scheme can be studied under fixed mobility with varying number of malicious nodes and varying mobility with varying number of malicious nodes. Also the study can be enhanced to address other malicious nodes attacks that are not included in this research.

REFERENCE

Abinaya, V. & D. S., (2016). Hop count based enhanced cooperative bait detection scheme to prevent cooperative black hole attacks in MANETs. *International Journal of Research and Application,* 7(2), pp. 253-260. 7 pages.

Boora, S. & Ohri, S., (2013). A survey of layer specific and cryptographic primitive attacks and their counter measures in MANETs. *International journal of P2P network trend and Technology (IJPTT),* 3(4).

Jiang-Ming Chan, Po-Chun Tsou, Isaac Woungang, Han-Chieh Chao and Ching-Feng Lai., (2014). Defending against collaborative attacks by malicious nodes in

MANETs: A cooperative bait detection approach. *IEE system journal.*

Foruuzan, B. A.,(2008). *Data communication and networking.* 4th ed. New York: McGraw Hill Inc.

Vishnu K. and Amos J Paul., (2010). Detection and removal of cooperative black hole gray hole attacks in MANETs. *international journal of computer application ,* 1(22).

Mohan M. and Ramakrishna M., (2015). A survey on secured cooperative bait detection approach for detecting malicious nodes in MANETs. *International journal of recent and innovative trends in computing and communication,* 13(3).

Bello Musa Yakubu, Mr. Pankaj Chajera and Dr. Ahmed Baita Garko., (2015). Advance secured method for data transmission in MANETs using RSA algorithm. *International journal of advance technology in engineering and science ,* 3(1).

A. Syeda Mustapha, Dr. C. Nelson Kennedy Babu and R. Kasthuri., (2016). Token ring based cooperative bait detection scheme for both selfish and malicious nodes attack in ad-hoc communication. *Middle east journal of scientific research,* 4(24).

PP, A.-J. & Chacko, B., (2013). ECBDS: Enhanced cooperative bait detecction scheme for preventing collaborative attacks in MANETS. *International journal of science and research,* 6(4).

Ramaswamy, S. et al., (2013). Prevention of cooperative black hole attacks in wireless ad-hoc networks. *International journal of innovative science engineering and technology ,* 3(3).

Rana, A., Rana, V. & Gupta, S., (2014). *EMAODV: Technique to prevent cooperative attacks in MANETs.* Mumbai, International conference on eco-friendly computing and communication system.

Suntana, S. A. & Kazi, S. B., (2015). Reverse tracing scheme to prevent cooperative attacks in MANETs. *International journal of emreging technology in computer science and electronics ,* 14(4).