Detecting Attacks and Providing Secure Transmission in MANET

[1]S.Sangavi Priyadarshini [2]Dr. N. Lakshmi Narasimman
[1]P.G Student [2]Professor and Head
[1,2]Department of Computer Science & Engineering
[1,2]K.L.N.College of Engineering, Pottapalayam, Sivagangai 630612, India

Abstract

MANET is a network that consists of mobile autonomous nodes often composed of mobile devices. Here the nodes must cooperate with each other to establish communication. Each node in the MANET acts as a router by cooperating with each other's to forward data packets. The presence of collaboration of malicious nodes may disrupt the routing processes and lead to network failures. The lack of infrastructure with dynamic topology may lead MANETs to be exposed to black hole attacks and gray hole attacks. If there are malicious nodes present in the MANET it may violate Security conditions and launch grey hole attacks and black hole attacks. This can be overcome by CBDS which is defined using DSR protocol which integrates both proactive and reactive defense architectures. CBDS uses the reverse tracing algorithm. A security algorithm is proposed to enhance security, increase and refine the throughput and increase the packet delivery ratio. The proposed security algorithm outperforms the CBDS scheme.
Keyword- Cooperative Bait Detection Scheme (CBDS), Black Hole Attacks, Gray Hole Attacks, Dynamic Source Routing (DSR), Mobile Adhoc Network (MANET), Security Algorithm, Encryption, Decryption

I. INTRODUCTION

The presence of collaboration of malicious nodes in the network may disrupt the routing processes leading to the malfunctioning of the network operations. The lack of infrastructure with dynamic topology feature of MANET makes it highly prone to attacks. In case of black hole attacks malicious nodes attract packets by a forged (Route Reply) RREP claiming that it has the shortest path from the source to destination, it then drops the packets without forwarding them. Gray hole attacks are similar to black hole attacks but here the malicious node is not initially found out, it turns malicious only at later time. Gray hole attacks and black hole attacks can be determined using the (Dynamic Source Routing) DSR which involves two main processes: route discovery and route maintenance. Route discovery is undertaken when the source needs a route to destination. Route maintenance is carried out when a malicious node is found in the path of the identified route, and then the source restarts the route discovery phase to find out another possible route from source to destination. Cryptographic technique performs the encryption and decryption mechanism for the data that has to be transmitted. The source node encrypts the data and forwards to the destination. After receiving the data, the destination node decrypts it and gives the acknowledgement to the source node. The detection mechanism will find the attackers in the routing process. The results will efficiently increase the network performance and provides secure transmission.

II. LITERATURE REVIEW

Kejun Liu and Jing Deng (2007) proposed An acknowledgment based approach for the detection of routing misbehaviour in MANETs. The aim is finding out the routing misbehaviours. Some selfish nodes may participate in the route discovery and route maintenance process and refuse to forward data packets. The protocol used here is DSR (Dynamic Source Routing).2ack scheme is used to send two hop acknowledgement packets in opposite direction. This method overcomes limited power transmission and receiver collisions. Watchdog scheme is based on passive overhearing. pathrater finds and lays a route from source to destination that doesn't contain misbehaving nodes by cooperating with routing protocols.

Varshney and Kashyap Balakrishnan (2010) an efficient way to avoid black hole and cooperative black hole attacks in wireless ad hoc networks .An intermediate node, which takes part in packet forwarding, may behave maliciously and drop packets which goes through it, instead of forwarding them to the following node. The protocol used here is AODV (Ad hoc On Demand Distance Vector). In merkle tree a security agent established by a hardware thread uses parallel multithreading architecture to detect cases of attacks-those exploiting AODV control messages RREQ and RREP messages. If any detection rule is violated, black hole attack is detected and malicious node is isolated and recorded to black list. Fidelity table is where every node in the MANET participating is assigned a fidelity level that acts as the measure of reliability of that node, in case if the fidelity level of any node drops to zero, it is considered to be a black hole node and is eliminated. It offers the advantage of being easy to deploy, the wireless ad hoc network paradigm. It does not seek to fit in an active route between a given source and destination.

Rongqing Zhang and Ling yang (2012) proposed a Joint Relay and Jammer Selection for Secure Two-Way Relay Networks. We investigate joint relay and jammer selection in two-way cooperative networks, consisting of two sources, a number of intermediate nodes, and one eavesdropper, with the constraints of physical layer security. Specifically, the proposed algorithms select two or three intermediate nodes to enhance security against the malicious eavesdropper. The protocols used are DF protocol (Decode and Forward) and AF protocol (Amplify and Forward).The jamming nodes are used to produce intentional interference at the eavesdropper nodes in different transmission phases. The physical layer security issues with secrecy constraints in two way schemes have not yet been well investigated.

Madhurya and subhashini (2014) proposed the Implementation of enhanced security algorithms in mobile adhoc network. The algorithm proposed here is disturbance detection algorithm. The algorithm combines features of symmetric and asymmetric key cryptography to provide data security and authentication. Circular rotations and initial permutations enhance the strength of the algorithm. Encryption is done to the message on the sender side using public key. After the receiver gets the encrypted message decryption is done using private key to get the original message. Performance of the network is increased. Throughput is obtained with high security.

Kahate and Chandure (2015) improved the authentication mechanism for using extended public key cryptography in mobile adhoc network the main aim of this work is to provide a secure data transmission between source and destination. It will authenticate the node and ensure the security of important routing information in AODV protocol. The algorithm used here is hybrid encryption algorithm. The public key and private key for each node is generated using RSA algorithm. The source node (S) and destination node (D) performs public key exchange using its private key. Encryption of message is done at 'S' and decryption of message is done at 'D'.Once the sender starts transmission, each node will generate its certificate. If any node which is not a member of transmission tries to get the packet by issuing a certificate, the node will be considered as an intruder and the certificate is bad. As security feature is concentrated much it minimizes delay and throughput.

III. EXISTING SYSTEM

The source node randomly selects an adjacent node which is used to bait malicious nodes and prevent them from participating in the routing process using a reverse tracing technique. It is assumed that when there is a significant drop in packet delivery ratio an alarm is sent from destination node to source node to trigger the detection mechanism. Identify all addresses of the nodes in the selected routing path from source to destination. The source node identifies all addresses of nodes in the selected routing path from source to destination after the source has received a RREP message the source node may not necessarily find out the intermediate nodes has the routing information to the destination or which has the RREP message, this may result in the source node sending the packets through the fake shortest path chosen by the malicious node which may lead to a black hole attack. To solve this issue, the function of HELLO message is added to the CBDS to help each node to identify which nodes are adjacent nodes within one hop.

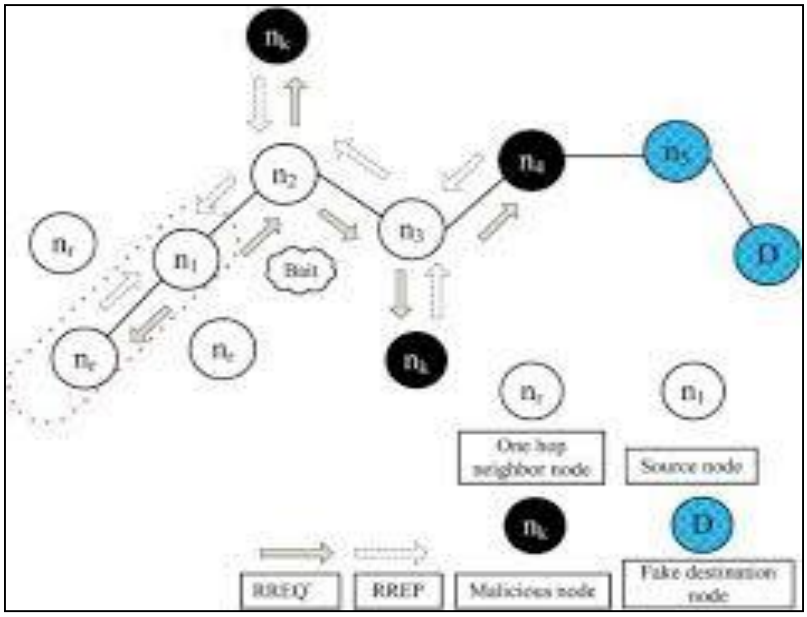

Fig. 1: Random selection of cooperative bait address

The CBDS scheme comprises of three steps 1) the initial bait step; 2) the initial reverse tracing step; 3) the shifted to reactive defence step. The first two steps apply the proactive methodology while the last step applies the reactive methodology.

In the initial bait step malicious node sends a RREP for the source node's RREQ' that it has the shortest path from source to destination. It gets the packets, retains them or drops it. Source node chooses the adjacent node (one hop) and fixes the bait's destination address in it to bait malicious nodes to send a RREP message. If nr node has not launched a black hole attack, source

node sends a RREQ', it will get RREPs in addition to that of nr nodes. Malicious nodes can be present in any of these routes. If nr node is the malicious node, it deliberately doesn't give any RREP and is blacklisted.

The initial reverse tracing step detects behaviour of malicious nodes through RREPs to RREQ' messages. Malicious nodes always reply with false RREPs. Reverse tracing program is conducted for the nodes which receive RREP from malicious nodes to delete temporarily trusted routes. CBDS must be capable of detecting more than one malicious node simultaneously.

Consider a malicious node nm replies with a false RREP, The node's address list is given as

$P=\{n_1 \ldots, n_k \ldots, n_m \ldots, n_r\}$

If another malicious node nk receives the RREP it will separate the address list as

$K_k = \{n_1 \ldots n_k\}$

K_k => route information from source node to n_k .

$$K_k' = P\text{-}K_k \{n_{k+1} \ldots n_m \ldots n_r\} \text{ ---- (1)}$$

Kk' => route information to the destination node.

On receiving the RREP n_k will compare 1) The source node's address in RREP.2) The next hop of n_k in P. 3) One hop of n_k.If A is not same as B and C then a recheck operation is done otherwise the packets are forwarded.

To obtain the trusted set 'T'

$$T = P - S\text{-----} \qquad (2)$$

In the shifted to reactive defense step the DSR route discovery process is activated. Route is established and if the packet delivery ratio from source to destination is lowered route maintenance phase is initiated.

IV. PROPOSED SYSTEM

In the proposed security algorithm, the cryptographic mechanism is used for providing packet security. This mechanism performs encryption and decryption process. A source node wants to transmit packet to the destination node. Using a simple hashing algorithm we get hashed value from a string of plain text. The hash value will be attached to packet header for data integrity checking. The following figure shows the process of encryption.

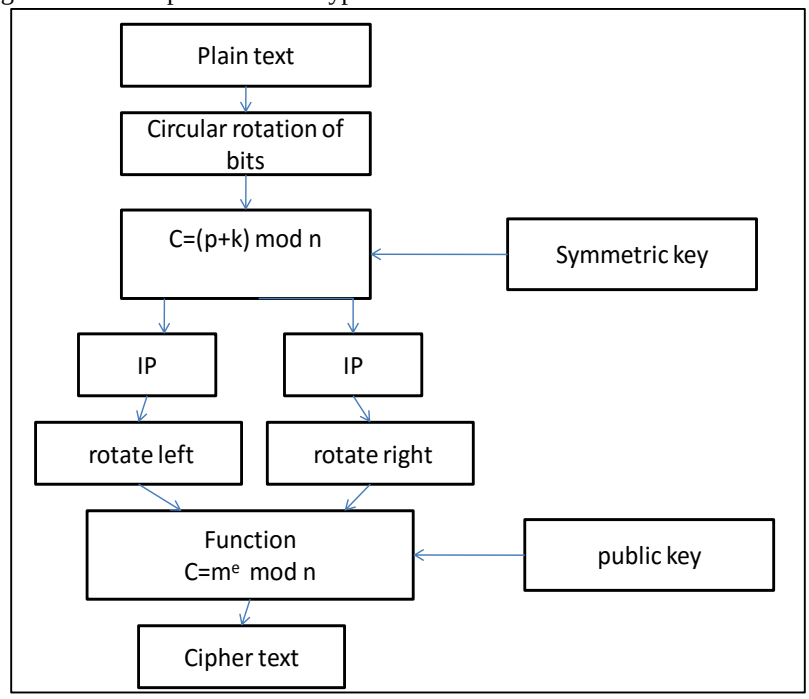

Fig. 2: Encryption

In the encryption process, plain text is a readable message or data that is fed into the algorithm as input. By performing circular rotation, bits can shift either left or right as per the requirement. Cipher text is a scrambled message produced as output which depends on plain text and the key. In this process the public key and private key are generated using RSA algorithm.

Select any two large prime numbers 'p' and 'q'

- Compute n= p*q
- Compute $\phi(n)=(p-1)(q-1)$
- Then $1<e<\phi(n)$, ('e' must be a prime number)
- Then $d.e \bmod \phi(n) =1$
- the public key is formed as $k_u =(e, n)$
- the private key is formed as $k_{r=}(d, n)$

The proposed security algorithm is a combination of RSA algorithm, caser cipher, rotations and permutations. As same the decryption process is performed which is shown in the following figure.

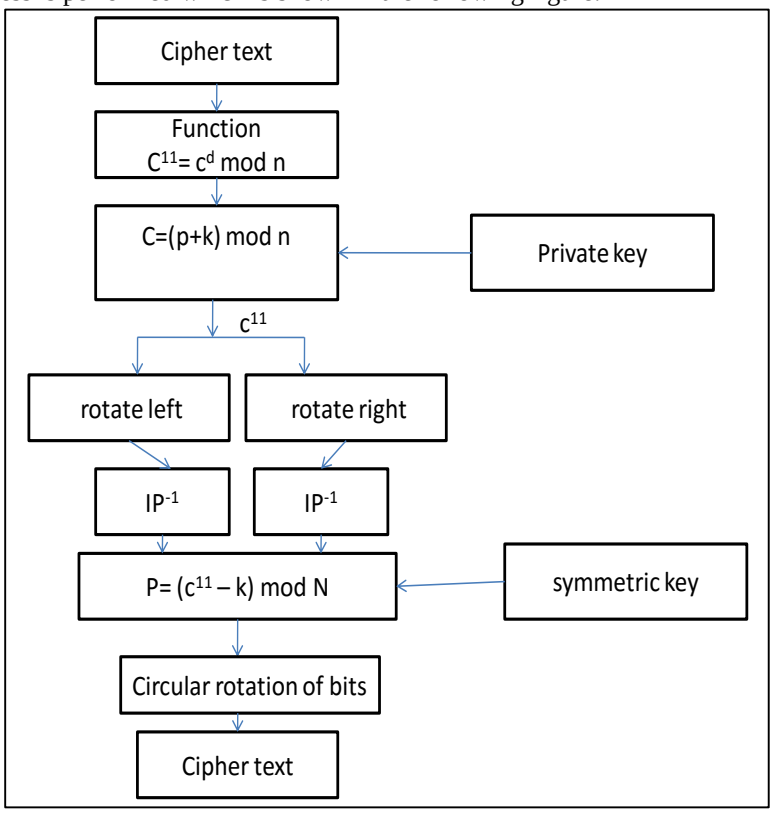

Fig. 3: Decryption

In the decryption process, the cipher text is converted into plain text. At the other end of communication, after decryption, the decrypted text will be hashed again to get new hashed value. This new hashed value will be compared to the value attached within packet header. If they are equal, the data integrity is ensured and decrypted text is accepted; otherwise the packet is discarded.

V. Conclusion

This paper introduces a new security algorithm which prevents the launching of black hole attacks and gray hole attacks. It helps in the safe and secure transmission of data from the source node to the destination node. It uses a novel encryption and decryption mechanism. It outperforms the existing CBDS scheme.

Acknowledgement

This work was supported in part by grants from the Dr. A.V. Ram Prasad, Principal of K.L.N. College of engineering and also supported by grants from DR.N. Lakshmi Narasimman, Professor & Head of Computer Science and Engineering (Project Guide), K.L.N. College of engineering, who had helped us during preparation and also provided valuable feedback for guidance.

References

[1] P.-C. Tsou, J.-M. Chang, H.-C. Chao and J.-L. Chen, “CBDS: A coopera-tive bait detection scheme to prevent malicious node for MANET based on hybrid defense architecture,” in Proc. 2nd Intl. Conf. Wireless Commun., VITAE, Chenai, India, Feb. 28–Mar., 03, 2011, pp. 1–5.
[2] S. Corson and J. Macker, RFC 2501, Mobile Ad hoc Networking (MANET): Routing Protocol Performance Issues and Evaluation Consid-erations, Jan. 1999. (Last retrieved March 18, 2013). [Online]. Available: http://www.elook.org/computing/rfc/rfc2501.html
[3] C. Chang, Y. Wang, and H. Chao, “An efficient Mesh-based core multicast routing protocol on MANETs,” J. Internet Technol., vol. 8, no. 2, pp. 229– 239, Apr. 2007.
[4] D. Johnson and D. Maltz, “Dynamic source routing in ad hoc wireless networks,” Mobile Comput., pp. 153–181, 1996.

[5] Rubin, A. Behzad, R. Zhang, H. Luo, and E. Caballero, "TBONE: A mobile-backbone protocol for ad hoc wireless networks," in Proc. IEEE Aerosp. Conf., 2002, vol. 6, pp.2727–2740.
[6] Baadache and A. Belmehdi, "Avoiding blackhole and cooperative blackhole attacks in wireless ad hoc networks," Intl. J. Comput. Sci. Inf. Security, vol. 7, no. 1, 2010.
[7] S. Marti, T. J. Giuli, K. Lai, and M. Baker, "Mitigating routing misbehav-ior in mobile ad hoc networks," in Proc. 6th Annu. Intl. Conf. MobiCom, 2000, pp. 255–265.
[8] K. Vishnu and A. J Paul, "Detection and removal of cooperative black/gray hole attack in mobile ad hoc networks," Int. J. Comput. Appl., vol. 1, no. 22, pp. 28–32, 2010.
[9] K. Liu, D. Pramod, K. Varshney, and K. Balakrishnan, "An Acknowledgement based approach for the detection of routing misbehavior in MANETs," IEEE Trans. Mobile Comput., vol. 6, no. 5, pp. 536–550, May 2007.
[10] H. Deng, W. Li, and D. Agrawal, "Routing security in wireless ad hoc network," IEEE Commun. Mag., vol. 40, no. 10, Oct. 2002.