A Reverse Tracing Scheme and Efficient Key Management for Secured Communication in MANET

K V Chaitra
Mtech, CNE
AMC Engineering College
Bangalore,India

J Selvin Paul Peter
Associate Professor, ISE Dept
AMC Engineering College
Bangalore,India

***Abstract*— Mobile ad-hoc network (MANET) consists of moving nodes which can design themselves without the inclusion of focal reconnaissance. The nodes communicate through remote medium including vicinity of intermediate nodes, impacts the network to different attacks on the ground that node can join and move the network any point of time. A predominant attack which lessens performance percentage is the blackhole attack. In this, the compromised node answers with false route to the destination and drops out the packets. A reverse tracing mechanism to detect and block the compromised nodes in network and secured communication with two level protection scheme is been underlined in this paper called as Reverse Tracing and Efficient Key Management (RTEKM). Dynamic Source Routing is been used to establish the route. Two keys participating in the proposed scheme are solitary. The key taking part in first level is generated from number of nodes involved in the route and the route request issued time. The Key Distribution Center provides the key which is imparted between source and the destination. The Reverse Tracing and Efficient Key Management (RTEKM) scheme introduced makes the manet an impregnable network**

***Key Words*— Blackhole attack, reverse tracing, dynamic source routing (DSR), Key Distribution Center(KDC), mobile ad-hoc network(MANET).**

I. INTRODUCTION

Mobile ad-hoc network consists of moving nodes which have the ability to configure themselves without the involvement of central surveillance. The nodes converse through wireless medium involving presence of intermediate nodes, influences the network to various kinds of attacks because node can join and move the network at any point of time. In mobile ad hoc networks (MANETs), for the establishments of communication among nodes in the network the nodes ought to participate with one other and nodes within the transmission range. Each node in a MANET is allowed to move autonomously in any direction, and will therefore the connectivity with other nodes will be evolving often. Because of this feature of manet, the network is presented to various attacks. When compared with wired networks where the nodes must have physical access to the network medium, mobile ad-hoc networks have no obvious secure limit. The attackers can communicate with all nodes once they are in the transmission scope of any other device. Henceforth security is the significant concern with the manet. Many research works have concentrated on the security of MANETS. The vast majority of them deal with prevention and detection approaches to combat individual misbehaving nodes. In this respect, the viability of these methodologies gets to be feeble at the point when different misbehaving nodes conspire together to launch a collaborative attack, which may result to all the more destroying harms to the network.

Due to the fluctuating topology, manets are vulnerable to different sorts of attacks. These attacks can disrupt the routing procedure. The most well-known and successive attacks in manet are blackhole attack, grayhole attack, jamming and data corruption. A blackhole attack or packet drop attack is a type of denial-of-service attack in which an intermediate node, that is supposed to relay packets, discards them. Grayhole attack is like slow poison. In this attack selective packets are dropped and remaining other packets are forwarded. Jamming is a kind of attack where the legitimate traffic is overpowered by illegitimate traffic. Data corruption occurs when transmitted data is been modified by hackers. In such environment there is a need for secure data transmission.

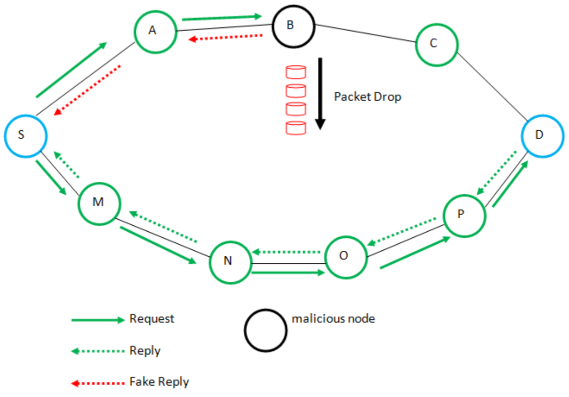

Fig. 1. Blackhole attack in manet

In manet typically when source broadcast the request all the other nodes in the vicinity of source receives the request and forwards to its neighbors. But in blackhole attack (see Fig. 1), the compromised node receives the request and it will not forward, instead it gives the fake shortest route to the destination. Source node when receives such reply chooses the shortest path involving the compromised node and transmit the packets. In turn, compromised node receives those packets and drops it. So to avoid such attacks an efficient scheme is required. In this paper a reverse tracing scheme is been used which detects and blocks the compromised node and also an efficient encryption scheme is been introduced which ensures data integrity and data confidentiality.

II. RELATED WORK

Many research works have explored the issue of malicious node recognition in MANETs. Majority of these solutions deals with discovery of a solitary malicious node or require enormous resources in terms of time and cost for recognizing cooperative blackhole attacks. In [1], Ali Belmehdi et al, proposed a secure mechanism, which comprises in checking the good forwarding of packets by an intermediate node The proposed solution evades the blackhole and the cooperative blackhole attacks. They proposed an answer, taking into account the standard of Merkle tree, for avoiding the blackhole and the cooperative blackhole attacks. Additionally, Gray hole, a variation of the blackhole, can undoubtedly be recognizable by their solution. In [2], Sergio Marti et al, presented two technique that improves throughput in ad-hoc network in the vicinity of nodes that concur to forward packets however failed to do as such. Watchdog is been used which identifies misbehaving nodes and path rater helps routing protocols to keep away from these nodes. When utilized together as a part of a network with moderate mobility, the two methods increment throughput by 17% in the vicinity of 40% misbehaving nodes, while expanding the rate of overhead transmissions from the standard routing protocols 9% to 17%. In [3], Vishnu K et al, introduced an attainable solution to recognize 2 sorts of malicious nodes (Black/Gray Hole) in the ad hoc network. The proposed solution can be connected to recognize and evacuate any number of BlackHole or GrayHole Nodes in a MANET and find a secure path from source to destination by evading the malicious nodes, In [4], Liu et al, proposed the 2ACK scheme that serves as an add-on technique for routing scheme to identify routing misbehavior and to alleviate their antagonistic impact. The fundamental thought of the 2ACK scheme is to send two-hop acknowledgment packets in the other way of the routing path. To diminish extra routing overhead, just a small amount of the received data packets are acknowledged in the 2ACK scheme. In [8], Xue et al, propose another routing service named best-effort fault-tolerant routing (BFTR).The outline objective of BFTR is to furnish packet routing service with high delivery proportion and low overhead in vicinity of misbehaving nodes. As opposed to judging whether a path is good or bad, i.e., whether it contains any misbehaving nodes, BFTR assesses the routing feasibility of a path by its end-to-end performance. By persistently observing the routing performance, BFTR dynamically routes packets by means of the most feasible path. BFTR gives a proficient and uniform solution for a wide scope of nodes misbehaviors a with exceptionally few security suppositions. In [9], Kozma et al, researched the issue of interestingly identifying the set of misbehaving nodes who decline to forward packets. We propose a novel misbehavior identification scheme called REAct that gives resource-efficient account- ability for node misbehavior. REAct identifies misbehaving nodes taking into account a series of random audits activated upon a performance drop. We demonstrate that a source-destination pair utilizing REAct can distinguish any number of autonomously misbehaving nodes based on behavioral confirmations gave by nodes. In this paper, a reverse tracing scheme is used which detects and block the compromised node and two level cryptographic scheme to provide security.

III. PROPOSED SYSTEM

In the proposed scheme (Fig. 2), a reverse tracing scheme is been utilized. The source chooses one of its one-hop neighbors as fake destination. The source then broadcast a request. In the event that there is a malicious node in the network, it gives a fake shortest route reply to the destination. The source then inspects the route replies and sends test packets. The route involving malicious node will not send the acknowledgment back to the source. Thus the source blocks the specific node and avoids the path involving the malicious node. Further to upgrade the security for the network a cryptographic scheme is been presented. This scheme includes two solitary keys. The data will be secured in two levels.

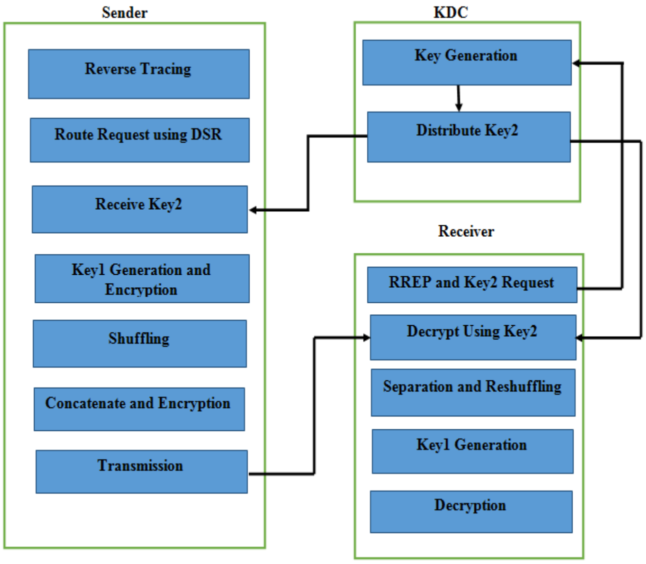

Fig. 2. System Architecture

A. *Reverse Tracing*

At first the source chooses one of its one-hop neighbor as the fake destination. Source then broadcasts the request containing fake destination address. On the off chance that the network is free from malicious nodes then source receives reply just from the one-hop destination. Assume there is a vicinity of maclicious node in the system then along with reply of destination, source additionally gets fake shortest route to the destination by malicious node. If in case the selected one-hop neighbor itself is malicious then it will not send the direct reply.

Since source node knows that it can directly communicate with the one-hop neighbor, when it receives reply from malicious node which gives shortest route, it identify it as malicious. Further to confirm source will send test packets to all the reply routes. Every node, when forwards the packet gives the acknowledgment back to the previous node and subsequently it is conveyed until the source. When malicious node receives the packets, it will drop the packets and will not give acknowledgment. This event is been notified by the healthy nodes involved in the route to the source. Further source notifies about the malicious node to all the neighbors and avoids the route involving malicious node.

B. Route SetUP

After notifying the neighbors about the malicious node, source broadcasts the request containing real destination address. Dynamic Source Routing algorithm (Table 1), which is an on-demand protocol is been used to establish the route. The intermediate node forwards the request and updates the route in the respective routing tables. Once the request reaches the destination, it gives the reply back.

TABLE 1
DYNAMIC SOURCE ROUTING ALGORITHM

```
Input:   RREQ
Output: RREP
BEGIN
Step 1: Source broadcast RREQ
Step2:  if (NODE==Destination)
          Send RREP to Source
          elseif (NODE==IntermediateNODE)
          Forward RREQ
Step3: if IntermediateNODE has DestinationInfo
         Send RREP to Source
Step4: if(NODE==Source)
         Receive RREP
         elseif (NODE==IntermediateNODE)
         Forward RREP
Step5: Update Route information
END
```

C. Key 2 Generation and Distribution by KDC

In this step, along with sending the reply to the source, destination also sends request to one of the multiple KDC present in the network which is near to it through intermediate nodes. The request contains address of source and the destination, The KDC will receive the request and generates a Key2. After the verification of source and destination the Key Distribution Center appropriates the Key2 directly to the source and the destination without involving intermediate nodes.

D. Key1 Generation and Encryption

Upon receiving the reply from destination and Key2 from KDC, source will choose the shortest route to the destination and generate Key1 using Key Generation algorithm (Table 2) which makes use of number of hops involved in the route and request sent time. Once the Key1 is been generated the source will encrypt the data using AES algorithm. At this stage the data will be encrypted for the first time. The obtained ciphertext is used for further processes.

TABLE 2
KEY GENERATION ALGORITHM

```
Input: Hour, Minute, Seconds, Hops
Output: Key1
BEGIN
 Step1:  if Hour is in single digit
           First bit=1
         else if Hour is double digit
           First bit=2
 Step2:  Concatenate First bit and Hour
           FirstBit+Hour
 Step3:  Concatenate result of Step 2 and Hops
           FirstBit+Hour+Hops
 Step4:  Multiply Hops with Minute
          Hops*Minute
 Step5:  Concatenate the result of Step 3with Step4
          FirstBit+Hour+Hops+(Hops*Minute)
 Step6: Multiply Hops with Second and
          concatenate with the result of Step 5
          (Hops*Seconds)+Step 5
 Step7: Convert the Hops into binary and
          concatenate with Step 6
 Step8: Append '0' with Step 7 to make Key1
          sixteen digit
 END
```

E. Shuffling and Concatenation

The number of hops and request sent time has to be sent to the destination in order to generate the first level key at destination side. To secure these values, shuffling algorithm is used where number of hops and request sent time is shuffled. The yield of the shuffling algorithm (Table 3) and the ciphertext obtained after encryption is concatenated.

TABLE 3
SHUFFLING ALGORITHM

```
Input: Hops, Hour, Minute, Second
Output: Shuffled Value
BEGIN
Step 1: Convert Hops, Hour, Minute and Seconds to
          binary value
Step 2: XOR the Hour and Minute
                 Hour XOR Minute
Step 3: XOR the result of Step 2 with Second
            (Hour XOR Minute) XOR Second
Step 4: Multiply Hops with the result of Step 3
          (  (Hour XOR Minute)XOR Second) * Hops
Step 5: Calculate the Log of the result of Step 4
           Log((  (Hour XOR Minute)XOR Second) * Hops)
END
```

F. Encryption and Transmission

The concatenated value is then encrypted using AES algorithm with the Key2 provided by KDC. The ciphertext is then transmitted via established path.

G. Decryption, Reshuffling and Decryption

After receiving the ciphertext the destination will decrypt it using the Key2 provided by KDC. Once the decryption is done the destination will be obtained with concatenated value (ciphertext and shuffled value).The value is separated and reshuffled. Using hops and the request sent time, the Key1 is once again generated using Key Generation algorithm. The destination makes use of Key1 to decrypt the ciphertext. The integrity and confidentiality of data is thus maintained.

IV. RESULT

We compare the existing DSR scheme with the proposed RTEKM based on the following performance factors

1) **End to End Delay:** It can be defined as the **time** taken for a packet to travel from the source to the destination. With the DSR scheme, where the security scheme is not been involved, end-to-end delay increases as the number of malicious nodes in the network increase. With RTEKM, number of malicious node decreases and hence decreases the end-to-end delay (see Fig. 3).

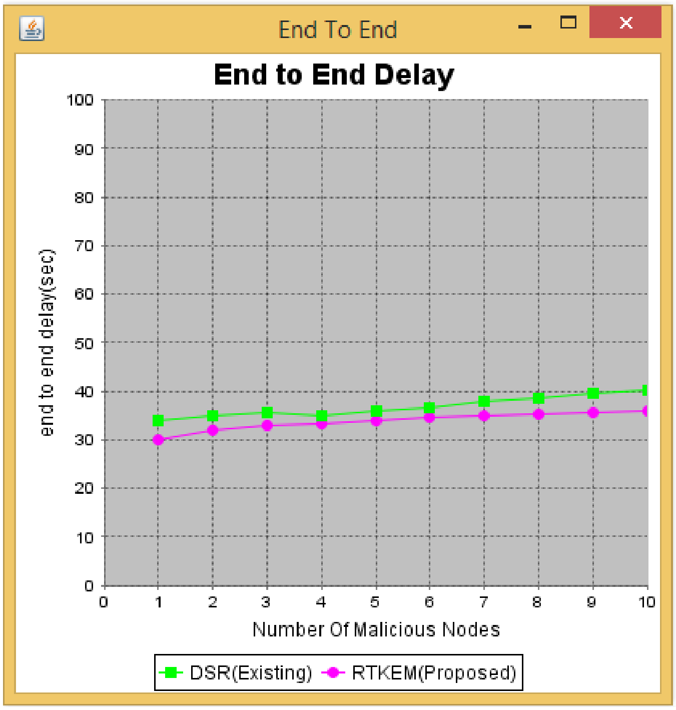

Fig. 3. End-to-End delay of DSR and RTEKM

2) **Packet Delivery Ratio:** This can be measured as total number of packets received by the destination to the total number of packets sent by the source. With DSR, the number of malicious nodes in the network is significantly more. The malicious nodes drops the packets instead of relaying it. Hence the total number of packets sent by the source may not reach the destination. As a result packet delivery ratio is lower. With the proposed RTEKM, malicious nodes are efficiently blocked. So the rate of packet delivery is greater when compared to DSR (see Fig. 4).

3) **Throughput:** It can be defined as ratio of total number of packets received by the destination from the source to the time it takes for the destination to receive the last packet. When compared with DSR, throughput is higher in RTEKM (see Fig. 5).

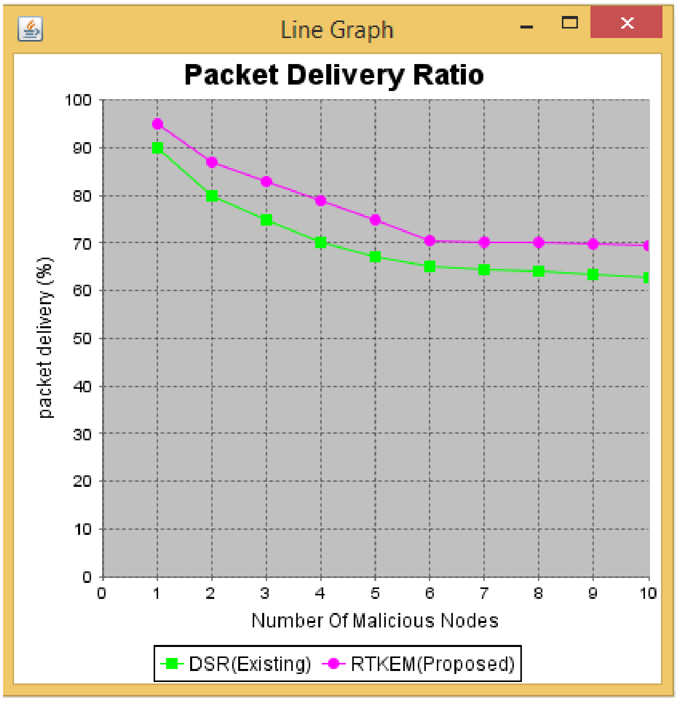

Fig. 4. Packet Delivery Ratio of DSR and RTEKM

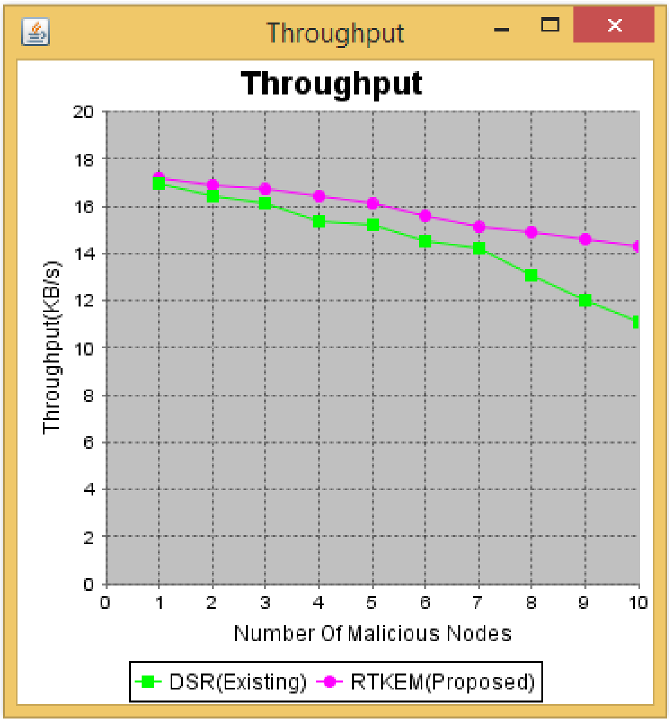

Fig. 5. Throughput of DSR and RTEKM

V. CONCLUSION

In this paper, a reverse tracing mechanism is been used which effectively identifies and blocks the nodes exhibiting blackhole attack. Further a protection scheme is been introduced which ensures security for the manet. The data will be encrypted in two levels. If suppose any one key is trade off, to obtain the original data intruder obliges another key. Thus with the scheme Reverse Tracing and Efficient Key Management (RTEKM), it is quite difficult to breach the integrity and confidentiality of the data. The experimental results shows that with the RTEKM, count of malicious nodes decrease gradually and network performance enhances.

REFERENCES

[1] 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.

[2] S. Marti, T. J. Giuli, K. Lai, and M. Baker, “Mitigating routing misbehavior in mobile ad hoc networks,” in *Proc. 6th Annu. Intl. Conf. MobiCom*, 2000, pp. 255–265

[3] 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

[4] 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

[5] W. Wang, B. Bhargava, and M. Linderman, “Defending against collaborative packet drop attacks on MANETs,” in *Proc.* 28*th IEEE Int. Symp. Reliable Distrib. Syst.*, New Delhi, India, Sep. 2009.

[6] S. Corson and J. Macker, RFC 2501, Mobile Ad hoc Networking(MANET): Routing Protocol Performance Issues and Evaluation Considerations, Jan. 1999. (Last retrieved March 18, 2013). [Online]. Available: http://www.elook.org/computing/rfc/rfc2501.html

[7] C. Chang, Y.Wang, and H. Chao, “An efficientMesh-based core multicast routing protocol onMANETs,” *J. Internet Technol.*, vol. 8, no. 2, pp. 229– 239, Apr. 2007

[8] Y. Xue and K. Nahrstedt, “Providing fault-tolerant ad hoc routing service in adversarial environments,” *Wireless Pers.Commun.*, vol. 29, pp. 367– 388, 2004.

[9] W. Kozma and L. Lazos, “REAct: resource-efficient accountability for node misbehavior in ad hoc networks based on random audits,” in *Proc. WiSec*, 2009, pp. 103–110.

[10] D. Johnson and D. Maltz, “Dynamic source routing in ad hoc wireless networks,” *Mobile Comput.*, pp. 153–181, 1996.

[11] I. Rubin, A. Behzad, R. Zhang, H. Luo, and E. Caballero, “TBONE: A mobile-backbone protocol for ad hoc wireless networks s,” in *Proc. IEEE Aerosp. Conf.*, 2002, vol. 6, pp. 2727–2740.

[12] H. Deng, W. Li, and D. Agrawal, “Routing security in wireless ad hoc network,” *IEEE Commun. Mag.*, vol. 40, no. 10, Oct. 2002.

[13] S. Ramaswamy, H. Fu, M. Sreekantaradhya, J. Dixon, and K. Nygard, “Prevention of cooperative blackhole attacks in wireless ad hoc networks,” in *Proc. Int. Conf. Wireless Netw.*, Jun. 2003, pp. 570–575.

[14] H. Weerasinghe and H. Fu, “Preventing cooperative blackhole attacks in mobile ad hoc networks: Simulation implementation and evaluation,” in *Proc. IEEE ICC*, 2007, pp. 362–367.