Context-free Protocol and N-ACK scheme for Secure Routing in MANET

Vani A.Hiremani[1], Snehal S. Jadhav[2]
Computer Department, Alard College of Engineering and Management, pune
[1]vani.hiremani@gmail.com
[2]jadhavsneha_9@yahoo.co.in

***Abstract*: Mobile Ad hoc Networks (MANETS) are transient networks of mobile nodes, connected through wireless links, without any fixed infrastructure or central management. Due to the self-configuring nature of these networks, the topology is highly dynamic. In general, routing protocols for MANETs are designed based on the assumption that all participating nodes are fully cooperative. Wireless Mobile ad hoc Networks suffer from a great efficiency loss due to the individual nodes that are constrained by the resources such as battery power and bandwidth. Misbehaving nodes makes the routing process a tedious task. One such routing misbehaviour is that some selfish nodes will participate in the route discovery and maintenance processes but refuse to forward data packets. A threat to such multihop transmission is posed by selfish nodes, which may drop others packets to save their own bandwidth and battery life. Therefore, packet forwarding is a fundamental problem for wireless ad hoc networks.This proposed method implements a context-free protocol that does not rely on observation and selfish behavior detection. Given a path, a context-free protocol can transmit packets through it without knowing whether the intermediate nodes are selfish or not. In this method, the data of a packet should be encrypted and the identity of the destination should only be revealed after all nodes forwarded the packet cooperatively. Multi hop acknowledgement N-ACK is used in this scheme to detect misbehaving nodes.**

***Keyword*: Context-free, Mobile Adhoc Networks (MANET), N-ack, Reputation based, Selfish node.**

I. INTRODUCTION

MANETs are formed by mobile nodes communicating with each other through wireless links without any governing body. In such a network nodes rely on each other to forward packets to remote destinations. The main area of consideration associated with the routing techniques that are employed for MANETS are the one that has the capacity to have ultra dynamic topology of the nodes and the requirement of each node to be routers themselves. The area of concern in this routing is when the nodes become selfish and tend to project its misbehaviour. An individual mobile node may attempt to benefit from other nodes, but refuse to share its own resources. Such nodes are called selfish or misbehaving nodes and their behaviour is termed selfishness or misbehaviour. This is a fundamental problem for ad hoc networks, and a lot of solutions have been proposed to stimulate nodes' cooperation.

Selfish node is a node which may deviate from the rules of cooperation, for example for the purpose of worsening network performance, similarly to what commonly occurs in denial of service attacks or in order to spare resources. Observing that if all nodes in a network cooperate with a given node, which does not cooperate with the other nodes, it gains the benefits of cooperation without consuming extra resources (energy) for cooperation with other nodes, and therefore is named selfish.

II. RELATED WORK

The techniques to combat node misbehaviour in MANETs are reputation-based. In such schemes network nodes collectively detect and declare the misbehaviour of a suspicious node. Such a declaration is then propagated throughout the network so that the misbehaving node will be cut off from the rest of the network. Several different protocols have been proposed for ad-hoc routing. The earliest protocols such as DSDV [04][07], DSR [04][07], and AODV [04]focused on problems that mobility presented to the accurate determination of routing information. DSDV is a proactive protocol requiring periodic updates of all the routing information. In contrast, DSR and AODV are reactive protocols, only used when new destinations are sought, a route breaks, or a route is no longer in use. While research has focused on "lightweight" security mechanisms, some proposed protocols use more expensive asymmetric cryptography. R.Balakrishna and U.Rajeswar Rao propose SAODV [03], a secure version of AODV, which uses digital signatures and hash chains to secure the routing messages. In [03], R.Balakrishna proposes a trust-based version of AODV using static trust levels. Neither of these addresses securing the trust exchanges, or the overhead involved. However, their protocol requires an intrusion detection system in the network.

Multipath routing allows use of multiple paths between from source to destination. There are three elements to multipath routing, namely path discovery, traffic distribution, and path maintenance. A lot of multipath routing protocols have been proposed for MANET where many of them are based on the famous distance vector routing and link state routing protocol [02]. P.Purniemaa proposes the Secure Message Transmission (SMT) protocol and Multipath Optimized Link state routing protocol (MP-OLSR) [02], which safeguards the data transmission against arbitrary malicious behavior of other nodes in multipath environment. Rizwan R. Rangara and Rupika S. Jaipuria introduce an intelligent secure routing model [06] for MANET. The intelligent model first detects the type of attack and chooses the optimum routing protocol according to the network attack using attack detection system (ADS).

Parkavi Murphy John and, Dr.P.Vivekanandan proposes Context free Protocol [01].That does not rely on observation and selfish behaviour detection. In this method, the data of a packet should be encrypted and the identity of the destination should only be revealed after all nodes forwarded the packet cooperatively. Context-free solutions introduce extra network traffic by modifying route paths. In this paper we propose context free protocol and N Ack scheme for secure routing in Manet.

III.Context Free Method

The main aim behind the Reputation based scheme is to detect selfish behavior of nodes and punish them in future. But context-free Method cannot detect the nodes behaviour, so the punishment cannot be in the future, but on the current packet transmission. This can be achieved by hiding the identity of the destination of the transmission. Along this, the methodology can be proposed for stimulating packet forwarding in a context-free way. First, the identity of the destination should be hidden. All nodes, including intermediate nodes and the destination node, have no way to reveal it during the forwarding stage.

There are two main ways for a node to know the destination of packet: the identity of the last hop of the route path and the data of the packet.

Therefore, two methods are needed:

• All information about route and destination should be removed from a packet.
• The data of a packet should be encrypted.

A. Protocol Design

The context free protocol is a complete context free solution for stimulating packet forwarding. Its basic idea is to hide the identity of the destination until all packet forwarding is done. To describe its design, we use the sample network in Fig. 1, in which node A is the source node, D is the destination, B, C, and N are other nodes in the network, and A-B-C-D is a route path.

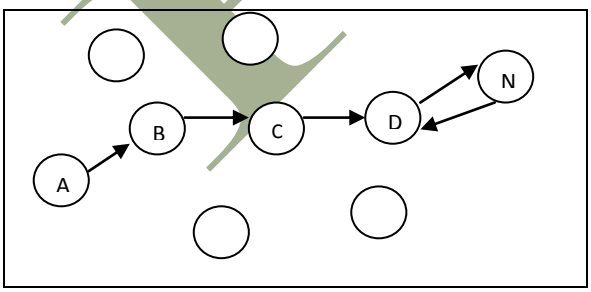

Fig 1.1 Routing in Context free Method

1 Context Free Path: As analyzed above, destination node D must also be an intermediate node. So in Context free method, source node A acquires D's neighbor node N, and changes the route path to a new path A-B-C-N-D, as shown in Fig. 1. Thus, the packet will arrive at the destination node twice.

2 Encryption: The data packet is encrypted by A with a randomly generated key K. Then key K is also encrypted with the public keys of all nodes on the route path in reverse order. So K is first encrypted with D's public key, then with N's public key, then D's public key again,

Then C's public key, and then B's public key .After such layered encryption, K can only be decrypted after nodes B, C, D, N, and D decrypt it with their secret keys one by one

Hash Key	Hash_cipher_path	Cipher Body

Fig 1.2 Context Free Packet

Please note that in a context free packet there is no information about the route path at all. Only A knows the path.

3 Packet Forwarding: Since there is no information about the route path at all, the Context Free packet is forwarded by broadcast. The receiving nodes decrypt the cipher-path and compare the result with hash key to see whether it is the destination, and compare with hash-cipher-path to see whether it is on the route path. If it is the destination, K can be decrypted out, and the packet's cipher body can be opened. If it is on the route path, update cipher-path to its decryption result and forward the packet; otherwise, drop it

IV. ROUTING ANALYSIS

If a source needs a route to a destination for which it does not already have a route in its cache:

• Source broadcasts Route Request (RREQ) message for specified destination
• Intermediate node Returns a route reply packet (RREP) (if route information about destination in its cache), or forwards the RREQ to its neighbors (if route information about destination not in its cache).
• If cannot respond to RREQ, increments hop count, saves info to implement a reverse path set up, to use when sending reply.
• RREQ packet contains: destination and source IP address, broadcast ID, source node's sequence number and destination node's sequence number. When Misbehaviour count is greater than the threshold for a node, information is sent to other nodes about misbehaving node.

A. Secure Routing

To provide security, routing divided issues into 3 categories:

• Key Exchange
• Secure Routing
• Data Protection

1 Key Exchange: All nodes before entering the network procure a one-time public and private key pair. After that, nodes can generate a Group Session Key between immediate neighbors using a suitable 'Group keying protocol'. These session keys are used for securing the routing process and data flow. Thus authentication, confidentiality and integrity are assured.

2 Secure Routing (RREQ): Node 'x' desiring to establish communication with 'y', establishes a group session key K_x between its immediate neighbors. After that it Creates RREQ packet, encrypts using K_x and broadcasts. Intermediate recipients that share K_x decrypt RREQ and modify. Intermediate nodes that do not share K_x initiate 'group session key exchange protocol' with the immediate neighbors. Intermediate nodes encrypt RREQ packet using the new session key and rebroadcast.

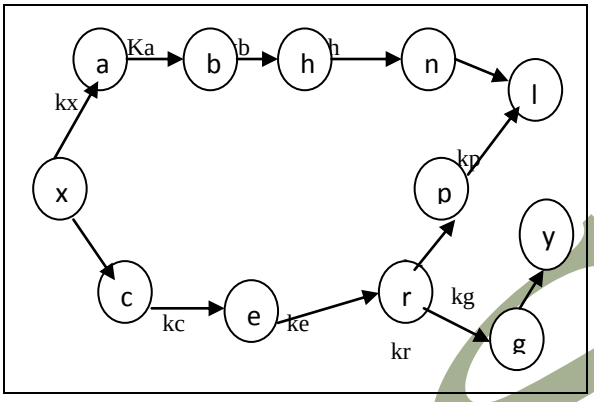

Fig 2.1 Key Exchange Encryption

3 Secure Routing (RREP): In response to RREQ, 'y' creates RREP.RREP is encrypted using the last Group session key that was used to decrypt RREQ and is unicast back to the original sender. If any of the intermediate nodes has moved out of wireless range, a new group session key is established. Recipient nodes that share the forward group session key decrypt RREP and modify. RREP is then encrypted using backward group session key and unicast to 'x'.

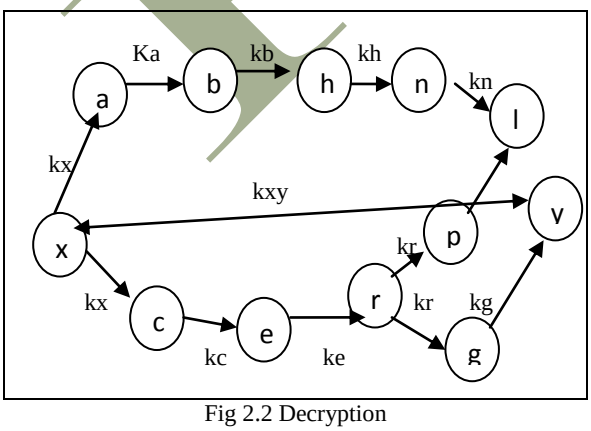

Fig 2.2 Decryption

4 Data Protection: Node 'x' desiring to establish end-to end secure data channel, first establishes a session key K_{xy} with 'y'.'x' symmetrically encrypts the data packet using K_{xy} and transmits it over the secure route. Intermediate nodes forward the packet in the intended direction. Node 'y' decrypts the encrypted data packet using K_{xy}.

V.CONTEXT FREE ROUTING

The target of Context free method is to make sure nothing leaks the identity of the destination. Here we introduce how it works. First, the Context free method packet body is encrypted, the key K is encrypted, and the other two parts are hashed results. Nothing can be used to imply the identity of the destination. Therefore, the nodes cannot get the identity of the destination from the packet itself. Second, in the Context free method path destination D appears twice. When D receives the packet for the first time, it cannot open the encrypted packet and does not know who is the destination. Now D has two choices: drop or forward. If D drops the packet, D loses its own data packet. Therefore, the rational way is to forward the packet. When another node such as C receives the packet, the situation is exactly the same. C is also not sure whether it is the final destination or not. So it will choose to forward the packet. Third, a special node involved in context free method is D's neighbor N. N receives the packet from D and then forwards it back to D. So can N guess that D is the destination? In fact it cannot, because in context free method, all forwarding is blind broadcasting. So when N forwards the packet, it does not know the downstream node is D. Therefore, N is not special in the context free path. Finally, people may have concerns about the loop at the end of the Context free path, which causes two extra hops in each transmission. But our study shows that it is infact not a big issue. Because context free nodes do not need to avoid selfish nodes, it can always make use of the best route path in the network.

VI.N-ACK SCHEME

The Nack scheme has a prerequisite of an end to end Ack packet to be sent between the source and the destination. The destination on receipt of the data packets sent by the source, responds with a Nack packet. Each node maintains a list of data packets sent and another list of data packets forwarded. As soon as a node initiates a data packet as a source, it adds the id of the packet to the list of data packet sent. As the node receives the Nack packet for the data packet it removes the corresponding data packet id from the data packet sent list.

The data packet and the Nack packet keep track of the route they travel. The Nack would try to reach the source from the destination with the help of the path, which is found in the actual message packet, delivered to the destination. If a node is found to be misbehaving in the pre calculated path, the

intermediate nodes are free to divert the Nack packet through alternative paths. But the new path will be stored in the Nack packet along with the older path, which is extracted from the original message.

On receipt of the Nack packet, the source node compares the two paths that are in the Nack packet. If there is no variation in the paths, then the source node concludes that there are no potential misbehaving nodes in the path. In case the two paths vary, the node in the source to destination path, from where the path varies in the destination to source path is isolated. This node is marked as a potential misbehaving node by the source node. For each potential misbehaving node, a threshold is maintained. If the number of times a node is adjudged as a potential misbehaving node exceeds the threshold, then the node is flagged as misbehaving and information is sent to all the neighboring nodes advising them about the misbehaving node. Further each node must send back a normal Ack to its immediate source node after receipt of any kind of packet. This would help the intermediate node to judge about its immediate neighboring node and advice the other nodes about the credibility of the neighboring nodes.

The process is similar to the protocol followed by a source node to keep track of data packets initiated. Here the intermediate nodes keep track of the forwarded data packets and Nack packets in the forwarded message packets list. The judgment of a neighboring node as potentially misbehaving node is done when an Ack is not received within a pre set time out.

As before, the number of times a neighboring is termed as potentially misbehaving node determines whether or not it should be termed as a misbehaving node. To consider the case in which the Nack packets are lost, the source node will wait for a certain time out period and then resend the original data packets assuming the data packets were lost.

On the other hand if the data packets are lost in the first case, the destination would receive the data packets for the first time during the subsequent retransmission by the source node and would respond to it. The combination of Nack and Ack for Nack is effective in isolating misbehaving nodes in a MANET.

A. Algorithm

- N1 the source has to send a packet to N5 the destination via N2->N3->N4.
- N1 adds the id of the packet to a wait list.
- N1 forwards the packet to N2 and waits for ack.
- If ack fails to arrive within the stipulated time N retries for K times after which it announces N2 to be misbehaving
- Then node N1 waits for the arrival of the N ack packet from the destination.
- It sets up a timer.
- Each intermediate node maintains a list of IDs for a data packet sent on a path.
- Each packet ID will stay for a time T.
- If Ack arrives within T, the ID is removed.
- Else ID will be removed after the timeout.
- N5 has to send back the N ack packet to the source.
- Each intermediate node has to forward the N ack packet to the source in the same path in which the initial transmission took place
- Each intermediate node also has to send to its immediate source node an ack packet
- Each node maintains a black list of potential misbehaving nodes
- If the ack is not received by a particular node then the node to which it has forwarded the packet and has failed to receive the ack is added to the list
- After K failed attempts to send the packet without receiving the ack - misbehaving node.

VII. CONCLUSION

Mobile Ad Hoc Networks (MANETs) have been an area for active research over the past few years due to their potentially widespread application in military and civilian communications. Such a network is highly dependent on the cooperation of all of its members to perform networking functions. The work is focused on routing path and encryption of packet and the key. Most existing solutions for stimulating packet forwarding in wireless ad hoc networks are context-based. They have some common components: observing nodes' behaviour, identifying selfish behaviours, and punishing selfish nodes. In this paper, we focus on cooperation in packet forwarding. a context-free protocol does not need to know whether nodes are selfish are not, and hence has no need to track nodes' behaviour to build a context, all the troubles caused by context maintenance no longer exist. Nack scheme is used for isolating misbehaving nodes in a MANET. Such a context-free solution is very different from traditional context-based ones and must be designed in a totally new way.

REFERENCES

[1] Parkavi Murphy John I, Dr.P.Vivekanandan **2**"A framework for Secure Routing in Mobile Ad hoc Networks ",IEEE-International Conference On Advances In Engineering, Science And Management (ICAESM - 2012) March 30, 31, 2012.

[2] 1P. Purniemaa, 2K. Manikandan, 3M.A.Saleem Durai "A Framework for Security Enhancement in Mobile-Ad-hoc Network" IJCST Vol. 2, Iss ue 2, June 2011.

[3] R.Balakrishna1, U.Rajeswar Rao2 , G.A.Ramachandra2 , M.S.Bhagyashekar3 "Trust-based Routing Security in MANETS"**,** R. Balakrishna et al. / (IJCSE) International Journal on Computer Science and Engineering Vol. 02, No. 03, 2010

[4] Rutvij H. Jhaveri1 , Ashish D. Patel2 , Jatin D. P,Bhavin I. Shah4 armar3 " MANET Routing Protocols and Wormhole Attack against AODV", IJCSNS International Journal of Computer Science and Network Security, VOL.10 No.4, April 2010

[5] M.N.Karuppusamy "Efficient Dynamic Nature Routing for Improving Node Lifetime in MANET ",International Journal of Advanced Information Science and Technology, Vol.8, Iss.8, Dec2012

[6] Rizwan R. Rangara ,Rupika S. Jaipuria ,Gauri N.Yenugwar1, Prof. P M. Jawandhiya2 " Intelligent Secure Routing Model For MANET " IEEE-2010.

[7] Karthik Sadasivam1 Vishal Changrani2 T. AndrewYang3 "Scenario based Performance evaluation of secure routing in MANET".

[8] Sumati Ramakrishna Gowda , P.S Hiremath "Secure Routing Schema for Manet with Probabilistic Node to Node forwarding" IJCSI International Journal of Computer Science Issues, Vol. 10, Issue 3, No 1, May 2013.

[9] Karim El Defrawy and Gene Tsudik "PRISM: Privacy-friendly Routing In Suspicious MANETs (and VANETs)" IEEE-2008.