International Journal of Emerging Technology and Advanced Engineering
Website: www.ijetae.com (ISSN 2250-2459 (Online), An ISO 9001:2008 Certified Journal, Volume 3, Special Issue 1, January 2013)

International Conference on Information Systems and Computing (ICISC-2013), INDIA.

SECURED CONSISTENT NETWORK FOR COPING UP WITH FABRICATION ATTACK IN MANET

P T Tharani[1], K Muthupriya[2], C Timotta[3]

[1,3] *Department of Computer Science and Engineering, PPG Institute of Technology,Anna University, Chennai, Tamil Nadu, India;*

[2] *Department of Information and Technology, PPG Institute of Technology, Anna University, Chennai, Tamil Nadu, India.*

[1]tharaniraj@gmail.com
[2]muthupriya.ciet@gmail.com
[1]ctimotta@gmail.com

Abstract

Recent advances in wireless communication along with peer –peer paradigm have led to increasing interest in P2P MANET. In mobile ad-hoc networks, mobile host move freely thereby disconnections occur frequently and result in network partition, which decreases data availability. Consequently, data replication improves data availability which maintains the consistency in network. MANETs must have a secure way for transmission and communication and this is a quite challenging and vital issue as there is increasing threats of attack on the Mobile Networks. In our approach, we present fabrication attacks against routing in ad hoc networks. It prevents attackers or compromised nodes from tampering with uncompromised routes consisting of uncompromised nodes, and also prevents attacks in MANET. In addition our protocol is efficient, using only highly efficient Asymmetric cryptographic primitives. In this paper we are using a secured routing protocol in a consistent network, which detects the malicious node and provides security to improve packet delivery ratio and to overcome the communication overhead in MANET. We also present the design and performance evaluation of a new secure routing protocol.

***Keywords*-- Consistency Management, Fabrication attack, Packet Delivery Ratio and MANET**

I. INTRODUCTION

In MANET partitioning of network takes place. To improve data availability, data replication is the solution. On this idea, authors have designed effective data replication techniques in MANETs in the previous papers [4, 5]. In [4], they have defined several different consistency levels for data operations on replicas in MANETs, and then, proposed Pessimistic protocols to realize them. For example, in Global Consistency the whole area is divided into several sub-areas called regions and proxies in the regions cooperatively behave in order to guarantee that every read operation on data items can read the replicas of the latest version. For this aim, the protocol of GC proposed in [4] uses the quorum system [8], which can perform read and write operations even if some mobile hosts that hold replicas disconnect from the network or network partitioning occurs. We have used a method [14], which divides the instances of each data item into multiple partitions and performs data operations locally on each partition to overcome the communication overhead and to increase the success ratio globally. MANET is vulnerable to various types of attacks because of open infrastructure, dynamic network topology, lack of central administration and limited battery-based energy of mobile nodes.

A common type of attacks targets at the underlying routing protocols. Malicious nodes have chance to modify or discard routing information or advertise false routes to attract user data to go through themselves. One such type is fabrication attack. In this type of attack a malicious node tries to inject fake messages or routing packets to disrupt the routing mechanism. These attacks are difficult to detect in a MANET since the routing packets appear to be legitimate packets to the nodes processing them. Some new routing protocols have been proposed to address the issue of securing routing information. In this work first we classify different attacks .Next we design a secured routing protocol with public key crypto system for improving global consistency and preventing fabrication attack in Mobile Ad-hoc network. We also report results to investigate the behavior of proposed protocol. It should be noted that our proposed protocols for achieving them are not very novel because these are basically common and simple approaches to maintain the consistency based on a typical quorum system.

The remainder of the paper is organized as follows: Section 2 contains related work, Section 3 describes classification of attacks, Section 4 describes our proposed work and section, 5 describes Results and conclusion.

International Journal of Emerging Technology and Advanced Engineering
Website: www.ijetae.com (ISSN 2250-2459 (Online), An ISO 9001:2008 Certified Journal, Volume 3, Special Issue 1, January 2013)
International Conference on Information Systems and Computing (ICISC-2013), INDIA.

II. Related Work

Quorum based consistency is a new field for research. Many researchers have contributed in the past in designing effective Global Consistency in MANET. In this section we briefly discuss some of the works they have done. Takahiro Hara et al [13] assumed special types of applications in which the instances of each data item can be partitioned and proposed two consistency management protocols which are combinations of an escrow method and their previously proposed protocols.Prashant Kumar et al [2] proposed a new proactive approach for cooperative caching in MANETs, in which they will cache the data of leaving node. Here each mobile node will broadcast a "LEAVE" message when it moves out from its zone. Based upon its Caching Information Table (CIT) zone manager will decide which data is to be cached. This will help to improve the data availability and overall performance of the network.T. Hara et al [4] aimed to discuss how to realize different types of consistency criteria in P2P MANETs. Since in P2P MANETs peers disappearance causes frequent network partitions, therefore, it is very difficult and in some cases even not desirable to provide traditional strict consistency among replicas. Moreover, since there are many kinds of applications possible in P2P MANET environments, there cannot be one universal optimal strategy for consistency management. S.K.Madria et al [4] explained different consistency levels and proposed protocols for achieving them and then they have discussed the impact of replica allocation for the system performance when the memory space of mobile host is limited. Aishwarya et al [1] Proposed approach that can be integrated on top of any source routing protocol and based on sending acknowledgement packets and counting the number of data packets of active path.

III. Network Layer Threats

Before entering into the details of our proposed scheme first let us characterize the network layer threats in brief.

- *Black hole:* In a black hole attack a malicious node advertises itself as having a valid route to the destination node even though the route is spurious. With this intension the attacker consumes or intercepts the packet without forwarding it. The attacker can completely suppress or modify the packet and generate fake information, which may cause network traffic diversion or packet drop.
- *Gray hole:* Gray hole is a node in the established routing topology that selectively drops packet with certain probability causing network distraction. Gray hole may drop packets coming from (or destined to) certain specific node(s) in the network while forwarding all the packets for other nodes. Another type of gray hole may behave maliciously for some time period by dropping all packets but may switch to normal behavior later. A gray hole may also exhibit a behavior which is a combination of the above two.
- *Worm hole:* A wormhole attack is where two or more malicious nodes may collaborate to encapsulate and exchange messages between them along existing data routes. The connectivity of the nodes that have established routes over the wormhole link is completely under the control of the two colluding attackers. A worm hole shows a valid route to the destination but it always tunnels the packet to its malicious partner node. This attack is also known as tunneling attack.
- *Jellyfish attack:* In jellyfish attack the malicious node first intrudes into the forwarding group in the network and then it reasonably delays data packets for some amount of time before forwarding them. This result in significantly high end to-end delay and delay jitter, and thus degrades the performance of real-time applications.
- *Spoofing:* This occurs when a malicious node pretends other node's identity at times. This in turn misguides a non malicious node in order to alter the vision of the network topology that it can gather.
- *Attacks using Fabrication:* In this type of attacks, a malicious node tries to inject fake messages or routing packets to disrupt the routing mechanism. These attacks are difficult to detect in a MANET since the routing packets appear to be legitimate packets to the nodes processing them. Figure.1 is an example of fabrication attacks. Node S wants to send data to node X, so it broadcasts a route request in order to find the route to node X.

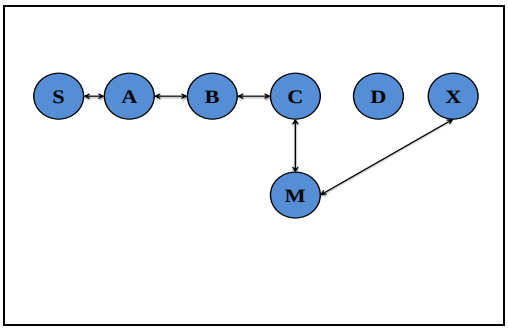

Fig. 1. Fabrication Attack in MANET

International Journal of Emerging Technology and Advanced Engineering
Website: www.ijetae.com (ISSN 2250-2459 (Online), An ISO 9001:2008 Certified Journal, Volume 3, Special Issue 1, January 2013)
International Conference on Information Systems and Computing (ICISC-2013), INDIA.

The Malicious node M pretends to have a cached route to the destination X, and returns route reply to the source node (S). The source node, without checking the validity of the RREP, accepts the RREP and starts to send data through M. Furthermore, malicious nodes can fabricate RERR to advertise a link break to a certain node in a MANET with AODV or DSR protocols.

- *Sybil attack:* In this attack, attacker pretends to have manifold identities/nodes. A malicious node can act as if it were a multiple number of nodes either by impersonating other nodes or simply by claiming false identities. This allows him to forge the result of a voting used for threshold security methods for more information.

IV. System Architecture

4.1 Proposed Model

Here we assume an area in which mobile hosts can move around is divided into several regions and the consistency of data operations on replicas is managed based on the regions.

The following notations are used in this paper.

- $R = \{R_1, R_2 \ldots R_l\}$ is the regions in the entire area.
- l is the total number of regions.
- R_r (r = 1,.., l) is the region identifier.
- M is the total number of mobile nodes.
- M_i (i = 1,.., m) is the host identifier.
- |QW| is the Quorum size for write operation.
- |QR| is the Quorum size for read operation.
- D_j is the Data item
- $|QLW_{ij}|$ is the Quorum size for write operation on data in the regions.
- $|QLR_{ij}|$ is the Quorum size for read operation on data in the regions.
- P_{ij} is the total number of peers that hold D_{ij} in the region.
- Each mobile host knows its current location by using some device such as GPS, and moves around in the given area. There are two kinds of mobile hosts: ***proxies and peers***.
- Proxy is a specially designated peer who manages other peers in a specific region in the MANET .Each proxy and peer knows all proxies in the entire network. This assumption is easy to find in many real situations. In an example of rescue service, it is natural that every member knows group leaders who act as proxies.
- Even when members do not know each other, a new peer has to register its participation to the proxy to join the MANET, and the peer can get the information on all proxies from the proxy. Here, every proxy can know all the others at the configuration phase of the MANET.
- A proxy has limited movement and does not go out of its region. Messages and data items are exchanged between peers using an underlying multi-hop routing protocol
- Each proxy maintains two tables,
- Mobile node's table, which has the information of all the mobile nodes within their regions, their unique id and address
- Neighbor proxy table, which has the information of adjacent proxy, their unique id and address.
- In a quorum system , read and write operations are performed only on replicas held by mobile hosts that form read and write quorums, respectively, where every pair of read and write quorums have an intersection.
- The consistency of data operations on replicas is managed at two levels: among peers in each region (local quorum) and among proxies (global quorum).
- The size of each global and local quorum is calculated to determine the consistency of the mobile host. The overview of global consistency and the message flow is proposed briefly in [4].

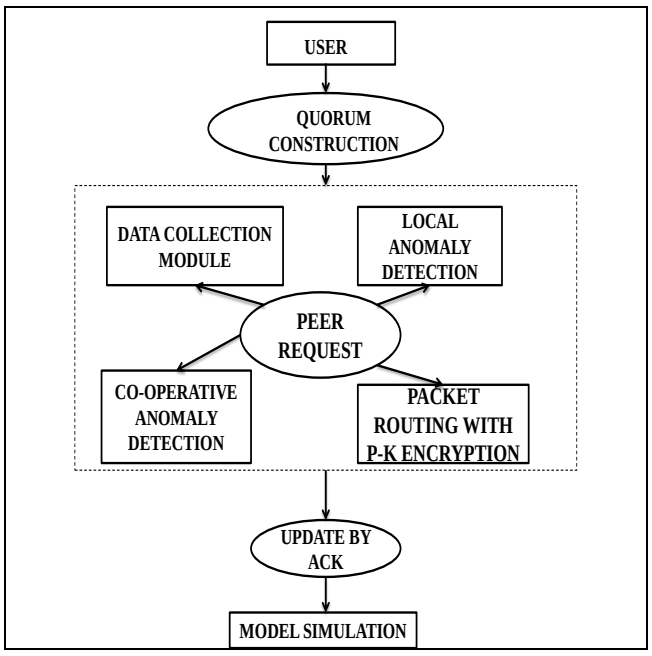

Fig . 2. System Architecture

International Journal of Emerging Technology and Advanced Engineering
Website: www.ijetae.com (ISSN 2250-2459 (Online), An ISO 9001:2008 Certified Journal, Volume 3, Special Issue 1, January 2013)
International Conference on Information Systems and Computing (ICISC-2013), INDIA.

- The selection should be LC rather GC in terms of both success ratio and traffic. So we have utilized the LC to increase data availability and to improve performance.

4.2 Quorum Construction

The Quorum is constructed based on the proposed method [13] where, each data item is partitioned into regions in MANET. Here, since we assume that a data operation consists of a pair of read and write operations, we use only one kind of the quorum size for a data operation, |QLrj|, which is different from the original LC protocol that uses two kinds of quorum sizes, |QLRrj| and |QLWrj|, for read and write operations.

The quorum size is determined by the condition $\mathbf{2X|QL_{rj}|>P_{rj}}$. Here $\mathbf{P_{rj}}$ is the total number of peers that hold a replica D_j in the region. The simplest way of setting this $\mathbf{|QL_{rj}|}$ as $\mathbf{QL_{rj} =[P_{rj} /2]+1}$. This also indicates the number of regions and the time stamp is assigned for each of the peer in the quorum.

4.3 The Protocol

The protocol is provided for the global consistent network as proposed in [14] where the instances of data item are replicated and divided into multiple partitions. This section briefly discusses the secured routing protocol for detecting the malicious node in network.

- Data collection module and Request to the peer
- Local anomaly Detection
- Co operative anomaly detection module
- Packet routing with Public key encryption
- Update with Acknowledgement

4.3.1 Data Collection Module and Request to the Peer

Table1.
DRI Table of Node A

NODE	FROM	THROUGH	RTS/ CTS	CHECK BIT
X	**0**	**0**	**15**	**0**
B	**1**	**1**	**5**	**1**
H	**0**	**1**	**3**	**0**
G	**1**	**0**	**6**	**1**
F	**0**	**1**	**4**	**0**

When a request is issued by the peer in region R4 to the peer in R6 for updating its peer with latest data item then peer in R6, sends request to the nearby proxy and peers of regions to accomplish the destination. Now proxy in region R6 checks whether the request has been sent from the valid mobile host. It now checks for the path from which the request has received.

Each node has information about its local peers and also the nearest proxies in the network. If the proxy is found to be secured then it sends the data, if not this phase fails. Now the proxy R4 routes the packet through our proposed protocol. Initially each node in the network collects the data forwarding information in its neighborhood and stores it in a table known as the *DATA ROUTING INFORMATION TABLE (DRI)*.

The DRI table of a node **A** maintains the packet routing information of its neighbor nodes **X, B, H, G** and **F**. An entry '1' for a node under the column '*from*' implies that node **A** has forwarded data packet coming from the node **X** nor it has forwarded any packet to the node **X**.However, node **A** has forwarded data packets to node **B** and also has forwarded data packets that have come from node **B**. In this way, each node constructs its DRI table and maintains it. After a certain threshold time interval, each node **identifies** its neighbor with whom it has not interacted for the purpose of data communication invokes subsequent detection procedure to explore them further.

This identification is done on the basis of the nodes that have '0' entries both in the '*from'* and '*through*' column in the DRI table 1. The RTS/CTS column in the DRI table gives the ratio of the number of the request to sent (RTS) message to the number of CLEAR to send message (CTS) for the corresponding node. This gives the rough idea about the amount of number of request arriving at the node for data communication and the number packet transmission that the node is actually doing. The significance of the column '*check bit'* in the DRI table will be discussed in the local anomaly detection procedure.

International Journal of Emerging Technology and Advanced Engineering
Website: www.ijetae.com (ISSN 2250-2459 (Online), An ISO 9001:2008 Certified Journal, Volume 3, Special Issue 1, January 2013)
International Conference on Information Systems and Computing (ICISC-2013), INDIA.

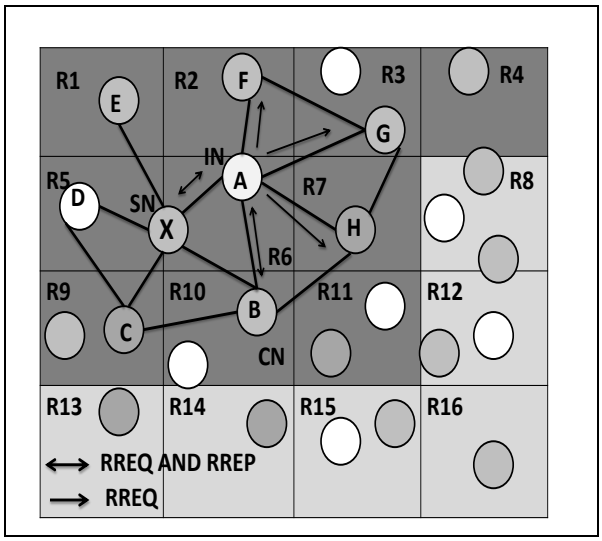

Fig. 3. Topology of MANET

4.3.2 Local Anomaly Detection

We call the node that initiates the local anomaly detection procedure as the initiator node (IN). The IN first chooses a cooperative node (CN) in its neighborhood based on its DRI records and broad casts a RREQ message to its 1-hop neighbor requesting for the route to CN. In the reply to this RREQ message the IN will receive a number of RREP messages from its neighboring nodes. It will certainly receive a RREP message from suspected node (SN) if the latter is really a malicious node. After receiving the RREP from the SN, the IN sends a probe packet to CN, through SN. After Time to Live (TTL) value of the probe packet is over, the IN enquires the CN, whether it has received the probe packet. In this reply to this query is positive, the IN node updates it DRI table by making entry 1 under the column '*check bit'* against the node ID of the SN. However, if the probe packet is found not to have reached the CN, the IN increases the level of suspension about the SN and activates the cooperative anomaly detection procedure.

In the Fig. 3, node **A** acts as the IN and initiates the local anomaly detection procedure for the SN (node **X**) and chooses node **B** as the CN. Node **B** is the most reliable node for the node **A** as both entries under columns 'From 'and 'Through' for node **B** is '1'. RREQ message is broadcasted by the node A to its entire neighbor node **X, B, H, G** and **F** requesting them for a route to the CN, i.e., node B in the example. After receiving a RREP from the SN (node **X**), node **A** sends a probe packet to the node **B** via node **X**. Node **A** enquires node **B** whether it has received the probe packet, node **A** makes an entry '1' under the column' *check bit'* in its DRI table corresponding to the row of node **X**.

If node has not received the probe packet, then node A invokes the cooperative local anomaly detection procedure.

4.3.3 Co-Operative Anomaly Detection Module:

The objective of this procedure is to increase the detection reliability by reducing the probability of false detection of local anomaly detection procedure. The procedure is activated when an IN observes that the probe packet it had sent to the CN through the SN did not reach the CN. The IN invokes the cooperative detection procedure and sends a cooperative detection request message, each of them sends a RREQ message to SN requesting for a route to the IN. After the SN responds with RREP message, each of requesting nodes sends a 'further probe packet' to the IN along that route. This route will obviously include SN, as SN is the neighbor of each requesting node and IN as well. Each neighbor of the SN except IN now notifies the IN that a 'further probe packet' has already been sent to it. This 'notification message' from each neighbor is sent to the IN through the routes which does not include SN.

Table 2.
Probe check table

NODE ID	PROBE STATUS
B	**0**
H	**1**
G	**1**
F	**1**

This is necessary to ensure that the SN is not aware about the on- going cross checking process. The IN will receive numerous 'further probe packets' and 'notification message'.

The IN now constructs a probe check table. The probe check table has two fields node id and probe status. Under the node id field, the IN enters the identifiers of the node which have sent the notification message to it. An entry of '1' is made under the column 'probe status' corresponding to the nodes from which the IN has received the 'further probe packet'. If further SN is found to behave like malicious node it is isolated from the network and message is sent to all nodes alarming the SN is found to be malicious node. Each time the peer updates itself with secured neighbour to route the packets.

International Journal of Emerging Technology and Advanced Engineering
Website: www.ijetae.com (ISSN 2250-2459 (Online), An ISO 9001:2008 Certified Journal, Volume 3, Special Issue 1, January 2013)
International Conference on Information Systems and Computing (ICISC-2013), INDIA.

4.3.4 Packet Routing With Public Key Encryption:

To ensure authenticity in the route the public key encryption is adopted for the peers in the DRI table. In public key cryptography each user or the device taking part in the communication have a pair of keys, a public key and a private key, and a set of operations associated with the keys to do the cryptographic operations. The distribution of public key is discussed in [14]. Now the node **A** has to reach mobile host in R4 which is the destination.

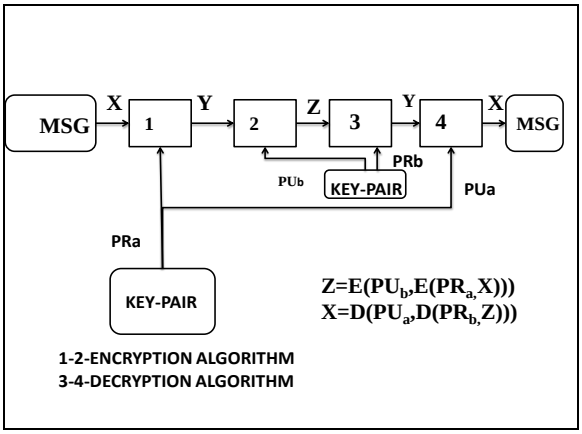

Fig. 4. Public key crypto system with Authentication and Secrecy

Now it can take the path from A- B- H- G- R4 or A-G-R4 and hence the shorter route A-G-R4 is considered. Suppose if the peer has to send data item to R-16, each peer taking part in routing the data item needs to check with the DRI table to route the packets. The Figure 4 illustrates the general use of the public key scheme to provide both the authentication function and confidentiality.

.

$$Z=E(PU_b,E(PR_g,E(PR_a,X)))$$

$$X=D(PU_a,D(PU_g,D(PR_b,Z)))$$

Fig. 5. Proposed Encryption Scheme

Figure 5, illustrates the encryption scheme. Now the peer prepares to route data item to Z in the region R4 and begins to encrypt the data item using sender's private key. This provides the digital signature. Next we encrypt again using receiver's public key. The final cipher text can be decrypted only by the intended receiver, who also has the matching private key. Thus, confidentiality is provided.

4.3.5 Update With Acknowledgment:

Each and every time the DRI table is updated by the IN node in the region and the malicious nodes is alarmed to the rest of the region. Now malicious node cannot inject fake messages or routing packets, since it is detected in the initial stage itself. The destination peer receives the data item. It decrypts the packet and updates the latest data items to all its peers in its region. The acknowledgement is also sent back to the sender peer.

V. RESULT ANALYSIS

We measured the Packet Delivery Ratio (It is defined as the output of total number of received data packets divided by the total number of sent packets), in an enough number of instances are available. This metric gives an estimate of how efficient a routing protocol is, since the number of routing packets sent per data packet gives an idea of how well the protocol keeps the routing information updated. We have compared PDR with proposed protocol with that of DSR routing protocol. The route fabrication attack will succeed with DSR cached route reply feature is enabled. When the number of malicious nodes increases, the number of received data packets decreases. Furthermore, DSR store the complete path to the destination. Hence, if any node moves out of the communication range, the whole route becomes invalid.

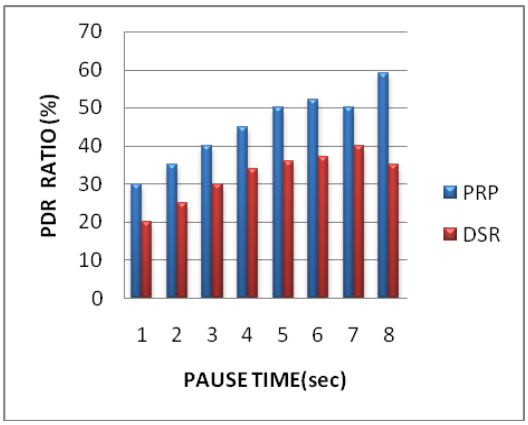

Fig. 6. PDR Ratio of proposed protocol

In MANETs, the nodes are mobile, so route change frequently occurs. Without being aware of most recent route changes, DSR may continue to send data packets along stale routes, leading to the increasing number of data packets being dropped. The PDR metric decreases when the number of malicious nodes increases.

International Journal of Emerging Technology and Advanced Engineering
Website: www.ijetae.com (ISSN 2250-2459 (Online), An ISO 9001:2008 Certified Journal, Volume 3, Special Issue 1, January 2013)
International Conference on Information Systems and Computing (ICISC-2013), INDIA.

Figure 6 illustrates the proposed routing protocol where PDR increases since it does not depend on the cache, it will trigger new route by detecting a new route. This shows proposed protocol remains high.

Fig 7 illustrates the Normalized Routing Load (NRL) (It is defined as the total number of routing packets sent divided by the total number of data packets received) which accounts for the overhead of the routing protocols. The number of total routing packets includes the number of route request packets (RREQ), route reply packets (RREP), route error packets (RERR), acknowledgement packets, hello protocol packets, etc.

This metric gives an estimate of how efficient a routing protocol is, since the number of routing packets sent per data packet gives an idea of how well the protocol keeps the routing information updated.

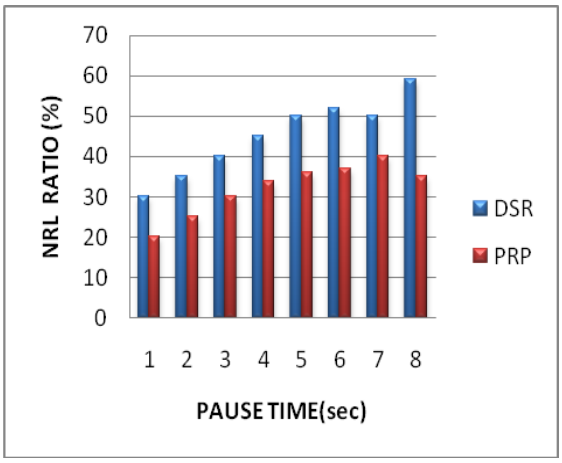

Fig. 7. NRL Ratio of proposed protocol

The higher the NRL metric is, the higher the overhead of routing packets and consequently the lower the efficiency of the protocol. The ratio of NRL is inversely proportional to the PDR. In our proposed protocol the NRL ratio is low compared to DSR protocol. For a route discovery to a destination, DSR will try more times, if no route reply is received.

In the case of route drop attacks, most of the routing packets dropped are RREQ, so the data source node keeps sending the RREQ until the number of RREQ retries reaches the maximum number. When the number of malicious node increases, the difference in routing packet sent is bigger. Furthermore, the number of received data packets is down with respect to the number of malicious nodes.

VI. CONCLUSION

In this paper we have presented a mechanism for detection of fabrication attack. Two metrics, Packet Delivery Ratio (PDR) and Normalized Routing Load (NRL), are used to estimate the protocols. Based on the results we've collected; we conclude that, in all the malicious environments, normal routing protocol (DSR) cannot guarantee to deliver data to the destinations as well as in the kind environments. In other words, the data is redirected or discarded due to the attacks on the routing protocol. When the number of malicious nodes increases, the number of received data packets decreases. For the secure versions of the routing protocols, we have designed our scheme to detect the changes in routing packets for consistent environment. It is expected that packet delivery ratio of data operations much improves even if the MANET is sparse, and the communication overhead for data operations is much reduced.

REFERENCES

[1] Aishwarya Sagar Anand Ukey, Meenu Chawla," Detection of Packet Dropping Attack Using Improved Acknowledgement Based Scheme in MANET", IJCSI International Journal of Computer Science Issues, Vol. 7, Issue 4, No.1, July 2010.

[2] Prashant Kumar, Naveen Chauhan, LK Awasthi, Narottam Chand," Proactive Approach for Cooperative Caching in Mobile Adhoc Networks" IJCSI International Journal of Computer Science Issues, Vol. 7, Issue 3, No 8, May 2010.

[3] G. S. Mamatha and Dr. S. C. Sharma "A New Combination Approach To Secure MANETS Against Attacks", International Journal of Wireless & Mobile Networks (IJWMN) Vol.2, No.4, November 2010.

[4] T.Hara and S.K Madria,"Consistency management strategies for data replication in mobile ad hoc networks," IEEE Transactions on Mobile Computing, to appear, 2009.

[5] T. Hara and S.K Madria, "Data replication for improving data accessibility in ad hoc networks," IEEE Transaction on Mobile Computing, Vol.5, No.11, pp.1515-1532, 2006.

[6] T. Hara and S.K. Madria, "Consistency Management among Replicas in Peer-to-Peer Mobile Ad Hoc Networks," Proc. IEEE Symposium. Reliable Distributed Systems (SRDS '05), pp. 3-12, 2005.

[7] L.D. Fife and L. Gruenwald, "Research issues for communication in mobile ad-hoc network database systems,"SIGMOD Record, Vol.32, No.2, pp.42-47, 2003.

[8] D. Malkhi, M.K. Reiter, and A. Wool, "Probabilistic quorum systems," Information and Computation vol.170, no. 2, pp. 184–206, 2001.

[9] Anita Vallur, Le Gruenwald, Nick Hunter, "REALM: Replication of Data for a Logical Group Based MANET Database," Proc. IEEE Workshop on Mobile Computing Systems, 2006.

[10] T. Hara, "Effective Replica Allocation in Ad Hoc Networks for Improving Data Accessibility," Proc. IEEE INFOCOM, pp. 1568-1576, 2001.

[11] D.B. Johnson, "Routing in ad hoc networks of mobile hosts,"Proc. IEEE Workshop on Mobile Computing Systems and Applications, pp.158-163, 1994.

[12] IETF MANET charter, http://www.ietf.org/html.charters/maneT-charter.html.

[13] Takahiro Hara," Escrow Approaches for Global Consistency in Mobile Ad Hoc Networks" International Conference on Complex, Intelligent and Software Intensive Systems.

[14] Salomaa, A. (1996), *Public-Key Cryptography* Springer-Verlag.

[15] K. Scott and N. Bambos, "The self-organizing wireless network (SWAN) protocol for communication among mobile users," Proc. IEEE Globcom' 95, pp.355-359, 1995.

[16] D.B. Johnson, "Routing in ad hoc networks of mobile hosts,"Proc. IEEE Workshop on Mobile Computing Systems and Applications, pp.158-163, 1994.

[17] Wenjia Li and Anupam Joshi ,"Security Issues in Mobile Ad Hoc Networks- A Survey".

[18] Jianmin Chen and Jie Wu ,"A Survey on Cryptography Applied to Secure Mobile Ad Hoc Networks and Wireless Sensor Networks".

[19] J. Grey, P. Helland, P.O'Neil and D. Shasha, "The Dangers of Replication and a Solution," Proc. ACM SIGMOD, pp. 173-182, 1997.

[20] Narayanan Krishnakumar And Arthur J.Bernstein, "Bounded Ignorance: A Technique for Increasing Concurrency in a Replicated System". ACM Transactions cm Database Systems, Vol 19, No. 4, December 1994.

[21] Rivka ladin and barbara liskovliuba shrira,"Providing High Availability Using Lazy Replication", ACM Transactions on Computer Systems, Vol. 10, No, 4, November 1992.

[22] Hector garcia-molina and daniel barbara, "How to Assign Votes in a Distributed System" Journal of the Association for Computing Machinery, Vol. 32, No. 4. October 1985, pp. 841-860.

[23] Anne Aaron and Jie Weng,"Performance Comparison of Ad-hoc Routing Protocols for Networks with Node Energy Constraints".

[24] Josh Broth David A. Maltz David B. Johnson Yih-Chun Hu,"A Performance Comparison of Multi-Hop Wireless Ad Hoc Network Routing", CopyrightACM19981-58113~35-i98110...S000.

[25] Michaelstonebraker,"Concurrency Control and Consistency of Multiple Copies of Data in Distributed INGRES", IEEE TRANSACTIONS ON SOFTWARE ENGINEERING, VOL. SE-5, NO. 3, MAY 1979.

[26] Robert H. Thomas,"A Majority Consensus Approach to Concurrency Control for Multiple Copy Databases", ACM Transactionso n DatabaseS ystemsV, ol. 4, No. 2, June 1979P, ages1 80-209.

[27] Ouri Wolfson and Amir Milo," The Multicast Policy and Its Relationship to Replicated Data Placement", ACM Transaction. on Database Systems, Vol 16, No 1, March 1991, Pages 1S1-205.

[28] Ouri Wolfsonl and Sushil Jajodia,"DISTRIBUTED ALGORITHMS FOR DYNAMIC REPLICATION OF DATA".

[29] Amr El Abbadi,Sam Toueg,"Availability in Partitioned Replicated Databases".

[30] Maurice Herlihy,"A Quorum-Consensus Replication Method for Abstract Data Types", ACM Transactions on Computer Systems, Vol. 4, No. 1, February 1986, Pages 32-53.

[31] Hector Garcia-Molina and Gio Wiederhold, "Read-Only Transactions in a Distributed Database", ACM Transactions on Database Systems, Vol. 7, No. 2, June 1982, Pages 209-234.

[32] Daniel Barbara, Member, IEEE, and Hector Garcia-Molina",The Reliability of Voting Mechanisms". IEEE TRANSACTIONS ON COMPUTERS, VOL. C-36, NO. 10, OCTOBER 1987.

[33] Michael J. Fischer and Alan Michael," sacrificing serializability to attain high availability of data in an unreliable network".

[34] Alan Demers, Karin Petersen, Mike Spreitzer, Douglas Terry, Marvin Theimer, Brent Welch, "The Bayou Architecture: Support for Data Sharing among Mobile Users".

[35] Jim Gray and Pat Helland and Patrick O'Neil,Dennis Shasha ,"The Dangers of Replication and a Solution".