FLEER: Faceless Location based Effective Expelling Rule in MANET's

V. Baskar, M. Kanakaraj, Dr. C. Kumar Charlie Paul

***Abstract*— A faceless effective rule used in Mobile ad hoc networks, shield the node identification and route from cradle to terminus. In existing expelling rules in MANET's are provide the encryption technique among in network so it generate the high cost for process or only provide one feature that is either faceless of cradle, terminus and route so it cannot provide full protection in network against the attacker. In this paper we introduce the Faceless location based effective expelling rule (FLEER). FLEER split the network into regions in between cradle to terminus and arbitrarily selects the race nodes between cradles to terminus and constructs the non-traceable faceless route. In addition FLEER mask the data initiator and receiver so it provide the efficient protection from intersection and timing attack in mobile ad hoc network. FLEER offer to provide full faceless of cradle, terminus and also route in network. FLEER reaches the better route faceless protection and also lowest cost compare to other faceless rule in mobile ad hoc network.**

***Index Terms*— Mobile ad hoc network, Faceless, Expelling rule.**

I. INTRODUCTION

Mobile ad-hoc networks (MANETS) has been very active, inspired mainly by allegedly important and numerous submissions in law enforcement, military and emergency response set-ups. More recently, location evidence has become increasingly available concluded small and budget GPS receivers. There is also an emerging trend to incorporate location-sensing into personal handheld devices .Combining ad hoc networking with location evidence facilitates some appealing new tenders, such as location-based advertising and focused dissemination of critical evidence. RAPID development of Mobile Ad Hoc Networks (MANETs) has inspired numerous wireless tenders that can be used in a wide number of areas such as commerce, emergency services, military, education, and entertainment. MANETs feature self-organizing and sovereign infrastructures, which make them an ideal optimal for uses such as communiqué and evidence sharing. Because of the openness and decentralization features of MANETs, it is usually not desirable to compel the member ship of the nodes in the network Compared to the wired networks Nodes in MANETs are vulnerable to malicious entities that aim to tinker and analyze data and traffic analysis by communiqué noise round or attacking expelling rules. Although anonymity may not be a requirement in civil oriented tenders, it is critical in military tenders (e.g., military communiqué). Consider a MANET deployed in a battlefield Anonymous routing protocols are crucial in MANETs to provide secure communiqués by hiding node identities and preventing traffic analysis attacks from outside onlookers. Faceless in MANETs includes identity and location Faceless of data cradles (i.e. forwarder) and For route Faceless, adversaries, either en route or out of the route, cannot trace a packet flow back to its cradle or terminus, and no node has evidence about the real identities and locations of intermediate nodes en route.

Also, in order to dissociate the relationship between cradle and terminus (i.e., relationship unobservability), it is important to form Faceless path between the two endpoints and ensure that nodes en route do not know where the endpoints are, especially in MANETs.

***Manuscript received Dec, 2013*.**

***V. Baskar**, Computer Science and Engineering, A.S.L Pauls College of Engineering and Technology, Coimbatore, India.*

***M. Kanakaraj**, Computer Science and Engineering, A.S.L Pauls College of Engineering and Technology, Coimbatore, India,*

***Dr. C. Kumar Charlie Paul**, Computer Science and Engineering, A.S.L Pauls College of Engineering and Technology, Coimbatore, India,*

II. RELATED WORK

Existing Faceless expelling rule in MANETs can be mainly classified into two parts one is hop-by-hop encryption and other one is redundant traffic. Most of the current approaches are limited by focusing on enforcing anonymity at a heavy cost to precious recalls because public-key-based encryption and high traffic generate significantly high cost. In addition, many approaches cannot provide all of the aforementioned Faceless protections. For example, ALARM cannot protect the location Faceless of cradle and terminus, SDDR cannot provide route Faceless, and ZAP only focuses on terminus Faceless.

Many Faceless expelling algorithms are based on the geographic routing protocol (e.g., Greedy Perimeter Stateless Routing (GPSR) that greedily forwards a packet to the node closest to the terminus. However, the protocol's strict relay node selection makes it easy to reveal the cradle and terminus and to analyze traffic. To provide high Faceless protection (for cradles, terminus, and route) with low cost, we propose a Faceless location based effective expelling rule (FLEER). FLEER split the network into regions in between cradle to terminus and arbitrarily selects the race nodes between cradles to terminus and constructs the non traceable faceless route.

Specifically, in each a data sender or forwarder panels the network field in order to separate itself and the terminus into two zones. It then randomly chooses anode in the other zone as then interlay node and uses the GPSR algorithm to send the data to the relay node. In the last step, the data is broadcasted to k nodes in the terminus zone, providing

ISSN: 2278 – 7798

k-anonymity to the terminus. In addition, FLEER has a strategy to mask the data initiator among a number of initiators to strengthen the Faceless protection of the cradle.

FLEER is also resilient to intersection attacks and timing attacks. We theoretically analyzed FLEER in terms of Faceless and effectiveness. We also conducted experiments to evaluate the performance of FLEER in comparison with other Faceless and geographic Expelling rules.

- FLEER provide route Faceless identity and location faceless of cradle, terminus and also provide route faceless
- To compare hop-by-hop encryption and redundant traffic, FLEER is uses randomized expelling of one message copy to provide faceless protection.
- Resolution to intersection attacks and timing attacks. FLEER has a strategy to effectively counter intersection attacks, which have proved to be a tough open issue. FLEER can also avoid timing attacks because of its non-fixed expelling paths for a cradle terminus pair.
- We construct comprehensive experiments to evaluate FLEER performance in comparison with other Faceless rules.

In this paper is organized as follows: In Section 2, we present the design of the FLEER expelling rule. Section 3 discusses the faceless performance of FLEER and its strategies to deal with certain attacks. In Section 4, we theoretically analyzed FLEER in terms of faceless and efficiency. Experimental performance of the FLEER rule is evaluated in Section 5. In Section 6, we describe related faceless expelling approaches in MANETs. The conclusion and future work are given in Section 7.

III. FLEER: FACELESS LOCATION –BASED EFFECTIVE EXPELLING PROTOCOL

A. Networks and Attack Models

FLEER can be applied to countless network models with countless node movement design such as random way point model and group mobility model. Consider a MANET positioned in a large field where geographic expelling is used for node communiqué in order to decrease the communiqué overhead. The location of a message's sender may be revealed by merely exposing the transmission direction. Therefore, a faceless communiqué rule that can provide un traceability is needed to strictly ensure the faceless of the sender when the sender communicates with the other side of the field. Moreover, a malicious observer may try to block the data packets by compromising a number of nodes, intercept the packets on a number of nodes, or even trace back to the sender by catching the data transmission direction. Therefore, the route should also be undetectable. A malicious observer may also try to detect terminus nodes through traffic analysis by launching an intersection attack. Therefore, the terminus node also needs the protection of faceless.

In this work, the attackers can be battery powered nodes that passively receive network packets and detect activities in their vicinity. They can also be powerful nodes that pretend to be legitimate nodes and inject packets to the network according to the analytical result s from their eavesdropped packets. The assumptions below apply to both inside and outside attackers. The nose round, the antagonist nodes can analyze any routing protocol and obtain evidence about the communiqué packets in their vicinity and positions of other nodes in the network. They can also monitor data transmission on the fly when a node is communicating with other nodes and record the historical communiqué of nodes. They can intrude on some specific vulnerable nodes to control their behavior, e.g., with denial-of-service (DoS) attacks, which may cut the expelling in existing faceless geographic expelling methods.

The attackers do not issue strong active attacks such as black hole. They can only perform intrusion to a proportion of all nodes. Their computing recradles are not unlimited; thus, both symmetric and public/private key cannot be brutally decrypted within a reasonable time period. Therefore, encrypted data are secure to a certain degree when the key is not known to the attackers.

B. Active anonym and position process

In one interaction of node communiqué, a cradle node S sends a request to a terminus node D and the terminus responds with data. A transmission session is the time period that S and D interact with each other continuously until they stop. In FLEER, each node uses a active anonym as its node identifier rather than using its real MAC address, which can be used to trace nodes' existence in the network. To avoid anonym traffic, we use a collision resistant hash function, such as SHA-1, to hash a node's MAC address and current time stamp. To prevent an attacker from re computing the anonym, the time stamp should be precise enough (e.g., nanoseconds). Considering the network delay, the attacker needs to compute, e.g., 10times for one packet per node. There may also be many nodes for an attacker to listen, so the computing overhead is not acceptable, and the success rate is low. To further make it more difficult for an attacker to compute the times tamp. Specifically, we keep the correctness of time stamp to a certain extent, say 1 second, and randomize the digits within 1/10th.

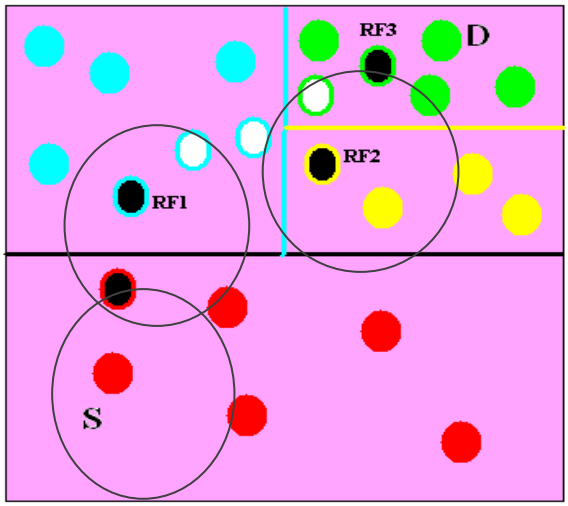

Fig1. Example for splitting regions in MANET's

As previous works, we assume that the public key and location of the terminus of a data transmission can be known by others, but its real identity requires protection. We can utilize a secure location service to provide the evidence of each node's location and public key. Such a location service enables a cradle node, which is aware of the identity of the

terminus node, to securely obtain the location and public key of the terminus node. The public key is used to enable two nodes to steadily establish a symmetric key Kfor secure communiqué. The terminus location enables a node to determine the next hop in geographic routing. The position-based routing systems depend on the position availability. It is assumed that a cradle is able to get the position of its terminus. The Global Positioning System (GPS) helps a node to get its own position. How a cradle gets the position of its terminus is a challenging task. In an ad hoc/cellular integrated environment [1], The position-based routing algorithms depend on the position availability. It is assumed that a cradle is able to get the position of its terminus. The Global Positioning System (GPS) helps a node to get its own position. How a cradle gets the position of its terminus is a challenging task. In an ad hoc/cellular integrated environment [2], the position of a terminus can be obtained through paging or the short message service through the cellular network. A cradle node sends a position request to the cellular position of a terminus can be obtained through paging or the short message service through the cellular network. A cradle node sends a position request to the cellular network. The cellular network pages the terminus. The terminus replies with its position, which is forwarded to the cradle. This *out-of-band* solution is simple since it has little signaling overhead and operational complexity. When an out-of-band server is not available, *d*eposition servers are designed. In [2], each node has a geographical region around a fixed center. The region is called a virtual home region (VHR) and the ad hoc node updates its network.

The cellular network pages the terminus. The terminus replies with its position, which is forwarded to the cradle. This *out-of-band* solution is simple since it has little signaling overhead and operational complexity. When an out-of-band server is not available, *in-band* position servers are designed. In [2], each node has a geographical region around a fixed center.

The region is called a virtual home region (VHR) and the ad hoc node updates its position evidence to all the nodes residing in its VHR.

Position evidence to all the nodes residing in its Specifically, trusted normal nodes or dedicated service provider nodes are used to provide location service. Each node has a location server. When a node A wants to know the location and public key of another node B , it will sign the request containing B's identity using its own identity.

Then, the location server of A will return an encrypted position of B and its public key, which can be decrypted by A using the pre distributed shared key between A and its location server. When node A moves, it will also periodically update its position to its location server.

IV. THE FLEER EXPELLING ALGORITHM

For ease of illustration, we assume the entire network area is generally a rectangle in which nodes are randomly disseminated. The evidence of the bottom-right and upper left boundary of the network area is configured into each node when it joins in the system. This evidence enables a node to locate the positions of nodes in the entire area for region panels in FLEER.

FLEER features a go-ahead and untraceable expelling path, which consists of a number of dynamically determined intermediate relay nodes. FLEER uses the hierarchical region partition and randomly chooses a node in the segregated region in each step as an intermediate relay node (i.e., data forwarder), thus vigorously generating an untraceable routing path for a message.

V. SIMULATION AND ANALYSIS

The Network Simulator ns-2.28 is used to analyse the system. The NS2 is a discrete event time driven simulator which is used to analyze the performance of a network.

The following parameters give the efficiency of the proposed system.

A. Packet Delivery Ratio:

The packet delivery ratio is one of the Quality of Service (QoS) metric to evaluate the performance of network. Low PDR depletes the network performance. Figure.2 shows that the proposed system has a good packet delivery ratio in spite of the channel assignment and rate re-assignment process.

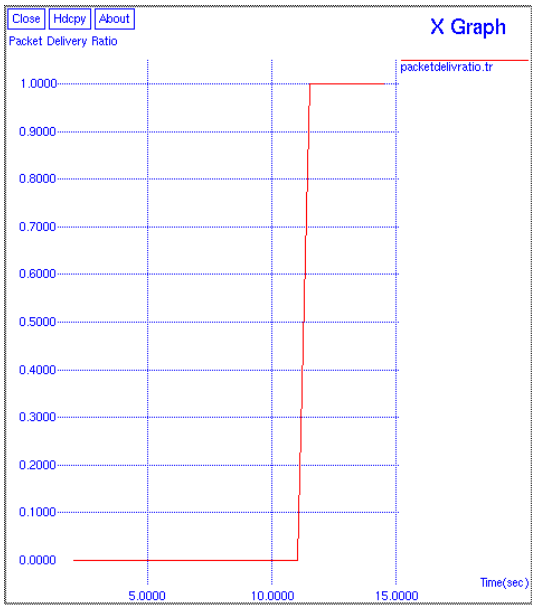

Fig2. Packet Delivery Ratio

During simulation time the events are traced by using the trace files. The performance of the network is evaluated by executing the trace files.

The events are recorded into trace files while executing record procedure. In this procedure, we trace the events like packet received, Packets lost, and delay etc. These trace values are write into the trace files.

This procedure is recursively called for every 0.05 ms. so, trace values recorded for every 0.05 ms. All the graphs obtained can be used to conclude that EMAP is efficient for the VANET operations.

B. Throughput:

In communiqué networks, such as Ethernet or packet radio, throughput or network throughput is the average rate

ISSN: 2278 – 7798

of *successful* message delivery over a communiqué channel. This data may be delivered over a physical or logical link.

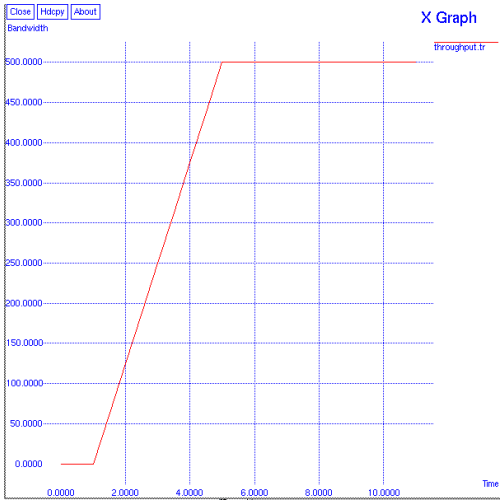

Fig2. Throughput

C. Packet Loss Ratio:

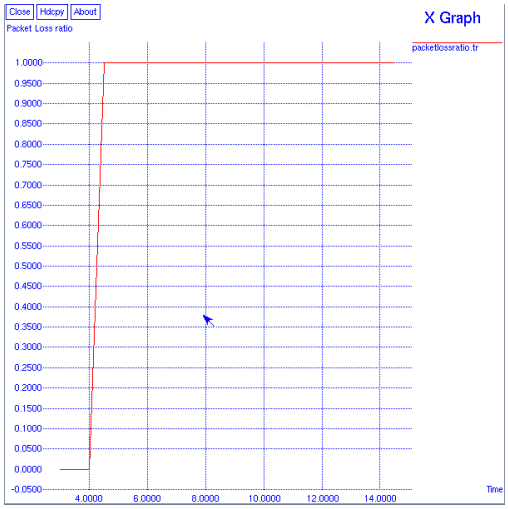

Fig4. Packet Loss Ratio

The Packet Loss ratio is the maximum number of packets possible to be dropped by a node. Figure 3 shows that the packet loss is minimized for the proposed scheme.

D. Packet Delay:

Packet Delay is the delay occurred during data transmission and it is given in figure 4.

The total delay taken for the packet transmission from cradle to terminus is shown in the above graph.

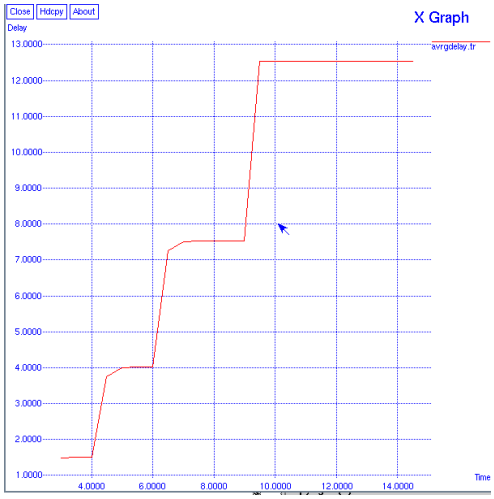

Fig 4. Packet Delay

E. Number of RFs:

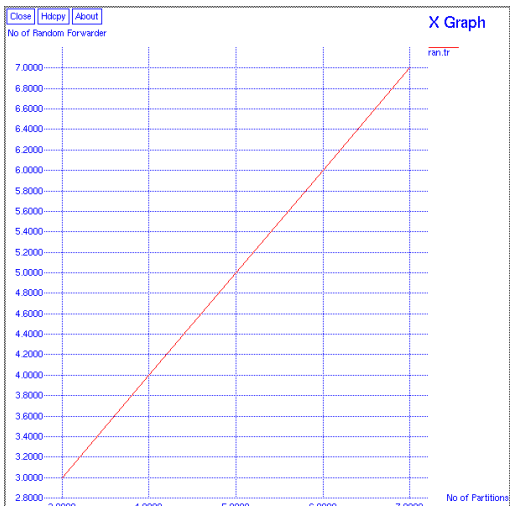

Fig 5. Number of Random Forwarders

The above Fig. shows the result versus the number of panels. We observe that the number of possible partitioning nodes exhibits a relatively faster increase when the number of panels H increases.

F. Anonymity

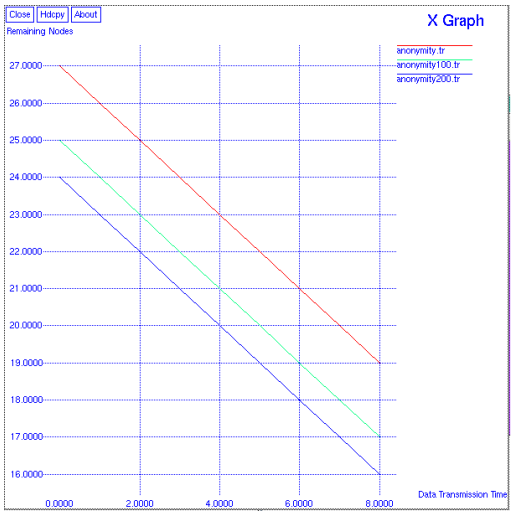

Fig 6. Anonymity

Above depicts the number of remaining nodes with five panels and a 2 m/s node moving speed when the node density equals 30, 100 and 200. The figure shows that the number of remaining nodes increases as node density grows while it decreases as time goes on.

This is because higher node density leads to more nodes in the terminus zone, and more nodes could remain in the terminus zone after certain a time than with lower node density. Also, because of node mobility, the number of nodes that have moved out of the terminus zone increases as time passes. This figure fits well with our analysis.

VI. CONCLUSION

FLEER is a routing protocol used to provide anonymity to cradle, terminus and the route of data transmissions. Unlike most other protocols, this is a low cost protocol that uses limited recradles yet provides security in the network. It uses dynamic hierarchical zone panels and random relay node selections to make it difficult for an intruder to detect the two endpoints and nodes en route. A packet in FLEER includes the cradle and terminus zones rather than their positions to provide anonymity protection to the cradle and the terminus. In addition, FLEER has an efficient solution to counter intersection attacks. FLEER's ability to fight against timing attacks is also analyzed. Simulation results show that FLEER can offer high anonymity protection at a low cost when compared to other anonymity algorithms.

REFERENCES

[1] A. Pfitzmann, M. Hansen, T. Dresden, and U. Kiel "Anonymity, Unlinkability, Unobservability, Pseudonymity, and Identity Management a Consolidated Proposal for Terminology, Version 0.31,"technical report, 2005.

[2] Sk.Md.M. Rahman, M. Mambo, A. Inomata, and E. Okamoto, "An Anonymous On-Demand Position-Based Routing in Mobile Ad Hoc Networks," Proc. Int'l Symp.Tenders on Internet (SAINT), 2006.

[3] Z. Zhi and Y.K. Choong, "Anonymizing Geographic Ad Hoc Routing for Preserving Location Privacy," Proc. Third Int'l WorkshopMobile Distributed Computing (ICDCSW), 2005.

[4] V. Pathak, D. Yao, and L. Iftode, "Securing Location Aware Services over VANET Using Geographical Secure Path Routing,"Proc. IEEE Int'l Conf. Vehicular Electronics and safety (ICVES), 2008.

[5] K.E. Defrawy and G. Tsudik, "ALARM: Anonymous Location-Aided Routing in Suspicious MANETs," Proc. IEEE Int'l Conf.Network Protocols (ICNP), 2007.

[6] K.E. Defrawy and G. Tsudik, "PRISM: Privacy-Friendly Routing in Suspicious MANETs (and VANETs)," Proc. IEEE Int'l Conf. Network Protocols (ICNP), 2008.

[7] Y.-C. Hu, A. Perrig, and D.B. Johnson, "Ariadne: A Secure On-Demand Routing Protocol for Ad Hoc Networks," Wireless Networks, vol. 11, pp. 21-38, 2005.

[8] I. Aad, C. Castelluccia, and J. Hubaux, "Packet Coding for Strong Anonymity in Ad Hoc Networks," Proc. Securecomm and Workshops, 2006.

[9] C.-C. Chou, D.S.L. Wei, C.-C. Jay Kuo, and K. Naik, "An Efficient Anonymous Communiqué Protocol for Peer-to-Peer Tenders over Mobile Ad-Hoc Networks," IEEE J. Selected Areas in Comm., vol. 25, no. 1, pp. 192-203, Jan. 2007.

[10] X. Wu, "AO2P: Ad Hoc On-Demand Position-Based Private Routing Protocol," IEEE Trans. Mobile Computing, vol. 4, no. 4,pp. 335-348, July/Aug. 2005.

V. BASKAR, revised the BE degree in Computer Science and Engineering from Anna University, Chennai, India, 2012. He is currently pursuing Master of Engineering in Computer Science and Engineering, A.S.L Pauls College of Engineering and Technology, Coimbatore, Tamilnadu, India. Research interests include Mobile Computing,, Cryptography and Network Security and Data Mining.

M. KANAKARAJ, Assistant Professor, Department of Computer Science and Engineering, A.S.L Pauls College of Engineering and Technology, Coimbatore, Tamilnadu, India.

DR. C. KUMAR CHARLIE PAUL, Principal, A.S.L Pauls College of Engineering and Technology, Coimbatore, Tamilnadu, India.

ISSN: 2278 – 7798