Volume 4, Issue 8, August 2014 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Reputation Based Alert Protocol for Mitigating Blackhole Attacks in Mobile Ad-Hoc Networks

Shubi K G*
CSE&Calicut University
India

Abstract*— *A mobile ad-hoc network is a self configuring infrastructure less network of mobile devices connected in a wireless manner. Anonymity is a state of being not identifiable within a set of subjects. MANETs make use of anonymous routing protocols in order to provide anonymity protection. Either hop-by-hop encryption or redundant traffic methods are used in existing anonymous routing protocols. But the existing protocols either generate high cost or cannot provide full anonymity protection. ALERT Anonymous Location Based Efficient Routing Protocol is a new protocol for providing high anonymity protection at low cost. In this protocol, network is portioned into zones in a dynamic manner. This protocol provides 1) source anonymity, 2) destination anonymity and 3) route anonymity. Simulation results of ALERT proves that this protocol performs better compared to existing protocols like GPSR. But still this protocol does not provide security to black hole attack. The objective of this research work is to overcome the pitfalls of the ALERT protocol and to develop a new protocol called R-ALERT which could withstand the blackhole attacks, using reputation mechanism.

Keywords*—*ALERT,anonymity protection,Blackhole attacks,R-ALERT

I. INTRODUCTION

A MANET is an autonomous collection of mobile users that communicate over relatively ―slow wireless links. The nodes are mobile. So the network topology may change swiftly and unpredictably over time. The network is decentralized. Thus all network activity, including discovering the topology and delivering messages must be accomplished by the nodes themselves. Each node in a wireless ad hoc network functions as both a host and a router, and the control of the network is distributed among the nodes. The network topology is in general dynamic, because the connectivity among the nodes may vary with time due to node departures, new node arrivals, and the possibility of having mobile nodes. An ad hoc wireless network should be able to handle the possibility of having mobile nodes, which will most likely increase the rate at which the network topology changes.

Each device in a MANET is free to move independently in any direction, and will therefore change its links to other devices frequently. Each must forward traffic unrelated to its own use, and therefore be a router. The primary challenge in building a MANET is equipping each device to continuously maintain the information required to properly route traffic. Such networks may operate by themselves or may be connected to the larger internet.

Opposed to infrastructure wireless networks where each user directly communicates with an access point or base station, a MANET, does not rely on fixed infrastructure for its operation. The network is autonomous transitory association of mobile nodes that communicate with each other over wireless links. Nodes that lie within each other's send range can communicate directly and are responsible for dynamically discovering each other. In order to enable communication between nodes that are not directly within each other's range, intermediate nodes act as routers that relay packets generated by other nodes to their destination. These nodes are often energy-constrained-that is, they are battery powered devices with great diversity in their capabilities. Furthermore, devices are free to join or leave the network and they may move randomly, possibly resulting in rapid and unpredictable topology changes. In the energy constrained dynamic, distributed multi-hop environment, nodes need to organise themselves dynamically in order to provide the necessary network functionality in the absence of fixed infrastructure or central administration. Despite the design constraints, mobile ad hoc networks offer numerous advantages. First of all, this type of network is highly suited for use in situations where a fixed infrastruure is not available, not trusted, too expensive or unreliable. Also, ad hoc networks do not need to operate in standalone fashion, but can be attached to the internet, thereby integrating many different devices and making their services available to other users. Furthermore, capacity range and energy arguments promote their use in tandem with existing cellular infrastructures as they can extend coverage and interconnectivity. As a consequence mobile ad hoc networks are expected to become an important part of the future 4G architecture which aims to provide pervasive computer environments that support users in accomplishing their tasks, accessing information and communicating anytime, anywhere and from any device.

Anonymous routing protocols are crucial in MANETs to provide secure communications by hiding node identities and preventing traffic analysis attacks from outside observers. Anonymity in MANETs includes identity and location anonymity of data sources and destinations as well as route anonymity. "Identity and location anonymity of sources

and destinations" means it is hard if possible for other nodes to obtain the real identities and exact locations of the sources and destinations. For route anonymity, adversaries, either in route or out of the route, cannot trace a packet flow back to its source or destination, and no node has information about the real identities and locations of intermediate nodes en route. Also, in order to dissociate the relationship between source and destination (i.e., relationship unobservability,) it is important to form an anonymous path between the two endpoints and ensure that nodes in route do not know where the endpoints are, especially in MANETs where location devices may be equipped.

In order to provide high anonymity protection (for sources, destination, and route) with low cost, an Anonymous Location-based and Efficient Routing protocol (ALERT), is proposed. ALERT dynamically partitions a network field into zones and randomly chooses nodes in zones as intermediate relay nodes, which form a no traceable anonymous route. Specifically, in each routing step, a data sender or forwarder partitions the network field in order to separate itself and the destination into two zones. It then randomly chooses a node in the other zone as the next relay 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 destination zone, providing k-anonymity to the destination. In addition, ALERT has a strategy to hide the data initiator among a number of initiators to strengthen the anonymity protection of the source. ALERT is also resilient to intersection attacks and timing attacks. But ALERT cannot prevent blackhole attacks. This research aims to mitigate the effects of blackhole attacks by using reputation mechanism.

II. RELATED STUDY

Jinyang Li John and Jannotti Douglas [1] has proposed Grid's Location Service (GLS) is a new distributed location service which tracks mobile node locations. GLS combined with geographic forwarding allows the construction of ad hoc mobile networks that scale to a larger number of nodes than possible with previous work. GLS is decentralized and runs on the mobile nodes themselves, requiring no fixed infrastructure. Each mobile node periodically updates a small set of other nodes (its location servers) with its current location. A node sends its position updates to its location servers without knowing their actual identities, assisted by a predefined ordering of node identifiers and a predefined geographic hierarchy. Queries for a mobile node's location also use the predefined identifier ordering and spatial hierarchy to find a location server for that node. Experiments using the ns simulator for up to 600 mobile nodes show that the storage and bandwidth requirements of GLS grow slowly with the size of the network. Furthermore, GLS tolerates node failures well: each failure has only a limited effect and query performance degrades gracefully as nodes fail and restart. The query performance of GLS is also relatively insensitive to node speeds. Simple geographic forwarding combined with GLS compares favourably with Dynamic Source Routing (DSR): in larger networks (over 200 nodes). This approach delivers more packets, and consumes fewer network resources.

Tomasz Ciszkowski and Zbigniew Kotulski[2] described that the pervasiveness of wireless communication gave mobile ad hoc networks (MANET) a significant researcher's attention, due to its innate capabilities of instant communication in many time and mission critical applications. However, its natural advantages of networking in civilian and military environments make them vulnerable to security threats. They proposed a new anonymous authentication protocol for mobile ad hoc networks enhanced with a distributed reputation system. The main objective was to provide mechanisms concealing a real identity of communicating nodes with an ability of resist to known attacks. The distributed reputation system is incorporated for a trust management and malicious behaviour detection in the network. The end-to-end anonymous authentication is conducted in three-pass handshake based on an asymmetric and symmetric key cryptography. After successfully finished authentication phase secure and multiple anonymous data channels are established. The anonymity is guaranteed by randomly chosen pseudonyms owned by a user. Nodes of the network are publicly identified and are independent of users' pseudonyms. They had also presented an example of the protocol implementation.

Yih-Chun Hu , David B. Johnson and Adrian Perrig[5] introduced SEAD that, an ad hoc network is a collection of wireless computers (nodes), communicating among themselves over possibly multihop paths, without the help of any infrastructure such as base stations or access points. Although many previous ad hoc network routing protocols have been based in part on distance vector approaches, they have generally assumed a trusted environment. The authors had designed and evaluated the Secure Efficient Ad hoc Distance vector routing protocol (SEAD), a secure ad hoc network routing protocol based on the design of the Destination-Sequenced Distance-Vector routing protocol. In order to support use with nodes of limited CPU processing capability, and to guard against Denial of- Service attacks in which an attacker attempts to cause other nodes to consume excess network bandwidth or processing time, they used efficient one-way hash functions and do not use asymmetric cryptographic operations in the protocol. SEAD performs well over the range of scenarios were tested, and is robust against multiple uncoordinated attackers creating incorrect routing state in any other node, even in spite of any active attackers or compromised nodes in the network.

Xiaoxin Wu and Bharat Bhargava[7],proposed that Privacy is needed in ad hoc networks. An ad hoc on-demand position-based private routing algorithm, called A02P, is proposed for communication anonymity. Only the position of the destination is exposed in the network for route discovery. To discover routes with the limited routing information, a receiver contention scheme is designed for determining the next hop. pseudo identifiers are used for data packet delivery after a route is established. Real identities (IDS) for the source nodes, the destination nodes, and the forwarding nodes in the end-to-end connections are kept private. Anonymity for a destination relies on the difficulty of matching a geographic position to a real node ID. That could be enforced by the use of secure position service systems. Node mobility enhances destination anonymity by making the match of a node ID with a position momentary. To further improve destination privacy, R-A02P is proposed. In the protocol, the position of a reference point, instead of the position of the destination,

is used for route discovery. Analytical models are developed for evaluating the delay in route discovery and the probability of route discovery failure. A simulator based on 77s-2 is developed for evaluating network throughput. Analysis and simulation results showed that, while A02P preserves communication privacy in ad hoc networks, its routing performance is comparable with other position-based routing algorithms.

Jiejun Kong and Xiaoyan Hong[9] presented that, In hostile environments, the enemy can launch traffic analysis against interceptable routing information embedded in routing messages and data packets. Allowing adversaries to trace network routes and infer the motion pattern of nodes at the end of those routes may pose a serious threat to covert operations. They proposed ANODR, an anonymous on-demand routing protocol for mobile ad hoc networks deployed in hostile environments. They addressed two closely related problems: For route anonymity, ANODR prevents strong adversaries from tracing a packet flow back to its source or destination; for location privacy, ANODR ensures that adversaries cannot discover the real identities of local transmitters. The design of ANODR is based on "broadcast with trapdoor information", a novel network security concept which includes features of two existing network and security mechanisms, namely "broadcast" and "trapdoor
information". They used simulations and implementation to validate the effectiveness of the design.

In the year 2006 Liu Yang, Markus Jakobsson and Susanne Wetzel[10] proposed that , recent years have seen a large number of proposals for anonymity mechanisms operating on the application layer. Given that anonymity is no stronger than its weakest link, such proposals are only meaningful if one can offer anonymity guarantees on the communication layer as well. ANODR – or Anonymous On Demand Routing – is one of the leading proposals to deal with this issue. The authors proposed a novel technique to address the same problem, but at a lower cost. The proposal, which they dub Discount-ANODR, is built around the same set of techniques as ANODR. Their proposal has the benefit of achieving substantially lower computation and communication complexities at the cost of a slight reduction of privacy guarantees. In particular, Discount-ANODR achieves source anonymity and routing privacy. A route is "blindly generated" by the intermediaries on the path between an anonymous source and an identified destination. Route requests in Discount-ANODR bear strong similarities to route requests in existing source routing protocols, with the limitation that intermediaries only know the destination of the request and the identity of the previous intermediary – but not whether the latter was the originator of the request. The response to a route request protects the compiled route by means of iterated symmetric encryption, drawing on how messages are prepared before being submitted to a typical synchronous mix network (or onion router). The communication of data subsequently uses such "route onions" to channel the packet to the intended destination. They didn't used any key exchange, nor used utilize public key operations at any time; consequently, they do not need to rely on any PKI, CRL or related constructions.

III. R-ALERT

The major issue identified in ALERT, is that it cannot prevent strong active attacks like black hole attacks. In networking , black hole refers to places in network where incoming or outgoing traffic is silently discarded without informing the source that the data did not reach its destination. Black hole attack makes the nodes to refuse in participating in the network activities when an established node drops out. All network traffics are redirected to a specific node, which does not exist at all that causes those data to be lost. This may even lead to reveal its security concerns. Black hole attack is one of the security threat in which the traffic is redirected to such a node that actually does not exist in the network.

A black hole attack in ad hoc networks refers to an attack by malicious nodes, which forcibly acquire the route from the source to destination by falsely advertising to reach the destination node. The malicious router can also accomplish this attack selectively, e.g. by dropping packets for a particular network destination, at a certain time of the day, a packet every n packets or every t seconds, or a randomly selected portion of the packets. This is rather called a gray hole attack. If the malicious router attempts to drop all packets that come in, the attack can actually be discovered fairly quickly through common networking tools such as trace route. Also, when other routers notice that the compromised router is dropping all traffic, they will generally begin to remove that router from their forwarding tables and eventually no traffic will flow to the attack. However, if the malicious router begins dropping packets on a specific time period or over every n packets, it is often harder to detect because some traffic still flows across the network. The objective of the research work is to implement a Reputation Based ALERT protocol for mitigating blackhole attacks and thereby to detect and prevent the black hole attacks.

In R-ALERT, a anonymous neighbor is selected for routing; but based on its reputation. In ALERT, a random node is selected as next hop by the GPSR protocol. But in R-ALERT, the reputation of the neighboring nodes will be monitored by the nearby nodes. When a node wants to transfer data, it uses GPSR to select a random nearest node to destination. In R-ALERT, a neighbor (random node which is in the communication range of a node) is selected , not randomly but based on reputation value.

$$\text{Reputation} = \frac{number\ of\ packets\ forwarded}{number\ of\ packets\ generated\ by\ own}$$

$$R_{ij} = \frac{\sum_{i=1}^{\infty} F_{ij}}{\sum S_{ij}}$$

Where, R_{ij} is the reputation of 'i' as seen by 'j'. F_{ij} is the number of the forwarded packets by 'i' and S_{ij} is the total number of packets generated by 'i'. R_{ij} will be calculated periodically. This R_{ij} value will be stored in a reputation table along with the neighbor id.

Table I
Reputation Table At A Node Say 10

Id	Reputation
1	0.8
2	0.4
3	0.6
4	0.3
5	0.5
6	0.7

IV. SIMULATION RESULTS

In this section, the simulation environment and the simulation results are discussed. Simulation is done using the network simulator NS-2. The number of nodes that have considered for is 50. One node is assumed to be an attacker, which is performing black hole attack. Connection type used is CBR to generate Constant Bit Rate data
Three parameters are used for evaluation of the proposed system. The parameters used here are Packet delivery ratio (pdr), Throughtput and Overhead

PACKET DELIVERY RATIO(pdr):
It is the ratio of the number of data packets delivered to the destinations to the number of data packets generated by the sources. This evaluates the ability of the protocol to deliver data packets to the destination in the presence of malicious nodes
This graph is taken by setting single malicious node in the scenario. This malicious node drops the packets which are passed through the node. The existing system is not able to cope up with malicious behaviour of mobile nodes. But the proposed system selects next hop for routing based on their reputation and hence the proposed system shows better pdr.

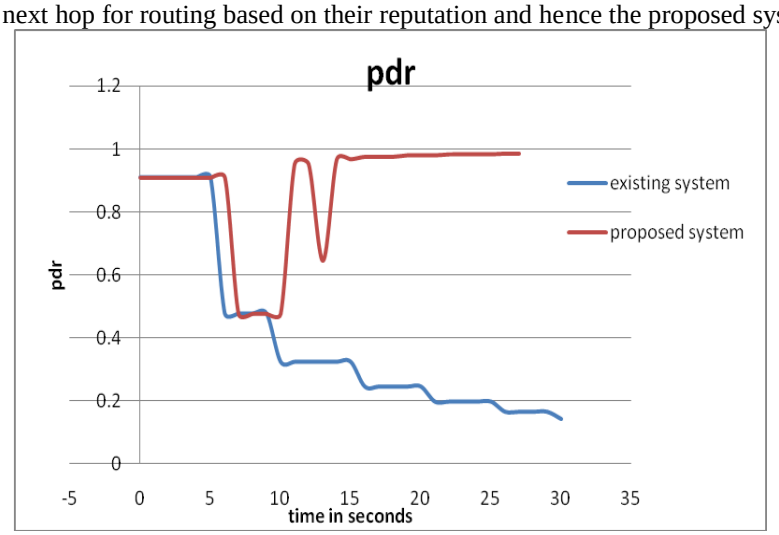

Fig 1: Packet delivery ratio

The malicious node is detected by the R-ALERT protocol. Instead of routing the data though the nodes with less reputation; R-ALERT selects the path based on high reputation value of the nodes. A path with highly reputed nodes is more reliable than a path with less reputed nodes. Since R-ALERT chooses next hops based on reputation of the neighbour , a reliable path is built. Thus PDR is maintained to be in a increased level.

THROUGHPUT
In communication networks, such as Ethernet or packet ratio, throughput or network throughput is the rate of successful message delivery over a communication channel. This data may be delivered over a physical or logical link, or pass through a certain network node. The throughput is usually measured in bits per second (bit/s or bps),and sometimes in data packets per second or data packets per time slot.

The fig 2 below shows the performance of throughput.

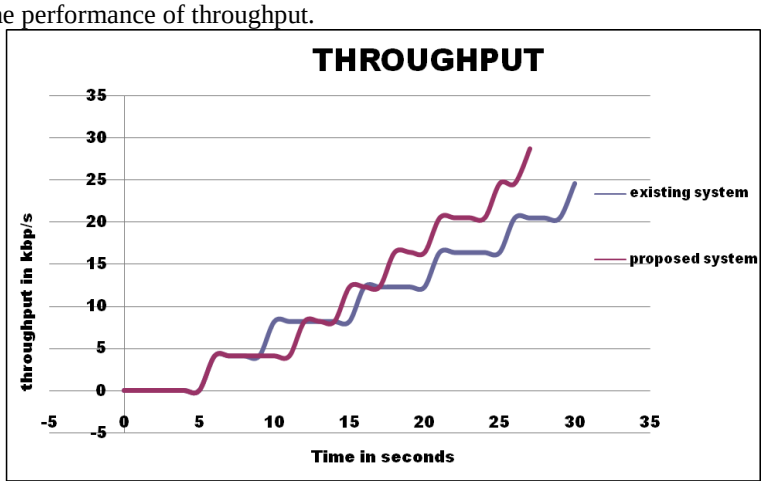

Fig 2: Throughput

The graph is plotted in terms of throughput and time in seconds. The graph helps to have a comparision of the existing work and the new approach.

OVERHEAD

Data that sent is across a wireless network is housed in a data envelope called a packet. Each transmission includes additional information, called overhead, that is required to route the data to the proper location. The overhead is calculted by sending a fixed-size data transmission across the network and observing the number of extra bytes of data transmission across the network and observing the number of extra bytes of dta transmitted for the action to be completed. The lesser the ovehead greater will be the efficiancy.

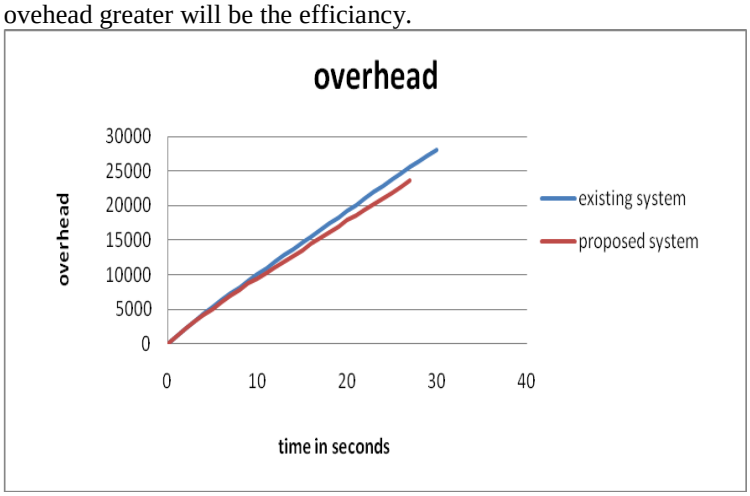

Fig 3 Overhead

The graph shows that the overhead has decreased in the proposed system compared to the existing system.

V. CONCLUSION AND FUTURE WORK

MANET, a mobile ad hoc network is a self configuring infrastructure network of mobile devices connected by wireless .A routing protocol specifies how routers communicate with each other. The anonymous routing protocols rely either on redundant traffic or on hop-by-hop encryption, generating high cost. Some of the protocols are also unable to provide complete source, destination and route anonymity protection. ALERT is distinguished by lower cost and offering anonymity protection for sources, destinations and routers. ALERT is not completely bulletproof to all attacks.It cannot fight against blackhole attack which is a serious attack in MANETs. Thus the blackhole attack detection and prevention mechanism has to be included in ALERT

The simulation results shows that the new approach reputation based ALERT protocol for mitigating blackhole attacks , provides better throughput,increased PDR and less overhead.

But in R-ALERT the notify and go phase introduces more overhead in terms of extra bytes transmission. This can be reduced by incorporating some simple mechanisms and will be carried out as a future work

ACKNOWLEDGMENT

The author gratefully acknowledge the support and facilities provided by Department of CSE, Vedavyasa Institute of Technology. Author also extend their thanks to the Head of the Department for the immense help during the course of the project.

REFERENCES

[1] J. Li, J. Jannotti, D.S.J. De, C. David, R. Karger, and R. Morris, "A Scalable Location Service for Geographic Ad Hoc Routing," Proc.ACM MobiCom, 2000.

[2] Tomasz Ciszkowski and Zbigniew Kotulski "ANAP:Anonymous Authentication Protocol In Mobile Ad hoc Networks ".

[3] G V Eswara Rao, D.Kamal Kumari and N.Krishna Santhosh,"CACS:Closed Anonymous Communication System For MANENTs ".

[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] Y.-C. Hu, D.B. Johnson, and A. Perrig, "SEAD: Secure Efficient Distance Vector Routing for Mobile Wireless Ad Hoc Networks," Proc. IEEE Workshop Mobile Computing Systems and Applications (WMCSA), 2002.

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

[7] 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.

[8] Y. Zhang, W. Liu, and W. Luo, "Anonymous Communications in Mobile Ad Hoc Networks," Proc. IEEE INFOCOM, 2005.

[9] J. Kong, X. Hong, and M. Gerla, "ANODR: Anonymous on Demand Routing Protocol with Untraceable Routes for Mobile Ad-Hoc Networks," Proc. ACM MobiHoc, pp. 291-302, 2003.

[10] L. Yang, M. Jakobsson, and S. Wetzel, "Discount Anonymous On Demand Routing for Mobile Ad Hoc Networks," Proc. Securecomm and Workshops, 2006.

[11] ALERT: An Anonymous Location-Based Efficient Routing Protocol in MANETs Haiying Shen, Member, IEEE, and Lianyu Zhao, Student Member, ieee. ieee transactions on mobile computing, vol. 12, no. 6, june 2013

