ISSN 2229-5518

Detecting Malicious Nodes For Secure Routing in MANETS Using Reputation Based Mechanism

Santhosh Krishna B.V, Mrs.Vallikannu A.L

ABSTRACT— Mobile ad-hoc networks (MANETS) are prone to a number of security threats. We incorporate our distributed reputation protocol within DSR and perform extensive simulations using a number of scenarios characterized by high node mobility, short pause time and highly sparse network in order to evaluate each of the design choices of our system. We focus on single and multiple black hole attacks but our design principles and results are applicable to a wider range of attacks such as gray hole, flooding attacks. Our implementation of black hole comprises active routing misbehavior and forwarding misbehavior. We design and build our prototype over DSR and test it in NS-2 in the presence of variable active black hole attacks in highly mobile and sparse networks.

INDEX TERMS: Black hole, Reputation, Flooding

1. INTRODUCTION

A mobile ad hoc network is a collection of wireless nodes that can dynamically be set up anywhere and anytime without using any pre-existing network infrastructure. It is an autonomous system in which mobile hosts connected by of wireless nodes that can dynamically be set up anywhere and anytime without using any pre-existing network infrastructure. It is an autonomous system in which mobile hosts connected by wireless links are free to move randomly and often act as routers at the same time; therefore, the limited wireless transmission range of each node gets extended by multihop packet forwarding.

This kind of network is well suited for the mission critical applications such as emergency relief, military operations, and terrorism response where no pre deployed infrastructure exits for communication. Due to its intrinsic nature of lacking of any centralized access control, secure boundaries (mobile nodes are free to join and leave and move inside the network) and limited resources mobile adhoc networks are vulnerable to several different types of passive and active attacks[1], [2]. Among these one of the most important security issues is the protection of the network layer from different active routing attacks. In this paper we tackled two types of routing attacks namely passive Black hole attack and active black hole attack which exhibits packet forwarding misbehavior. In a black hole attack malicious node (called black hole) replies to every route request by falsely claiming that it has a fresh enough route to the destination. In this way all the traffic of the network are redirected to that malicious node which then dumps them all.

1.1 BLACKHOLE ATTACK

A black hole is a node that always responds positively with a RREP message to every RREQ, even though it does not really have a valid route to the destination node. When the data packets routed by the source node reach the black hole node, it drops the packets rather than forwarding them to the destination node. Such malicious node also

advertises itself as having shortest path to requested node. In *fig. 1.1*, node 1 wants to send data packets to node 4 and initiates the route discovery process. We assume that node 3 is a malicious node and it claims that it has route to the destination whenever it receives RREQ packets, and immediately sends the response to node 1. If the response from the node 3 reaches first to node 1 then node 1 thinks that the route discovery is complete, ignores all other reply messages and begins to send data packets to node 3. As a result, all packets through the malicious node is consumed or lost.

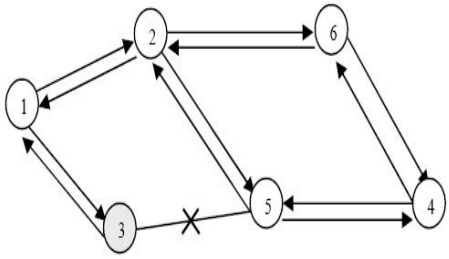

Figure 1.1 Black-hole attacks

Paper Outline

The rest of the paper is organized as follows. Related works is discussed in section 2. Our reputation based security protocol is discussed in section 3.reputation output in section 4, malicious node detection as section 5 and conclusion and future work as 6 and finally references as the last part.

2. RELATED WORKS

Distributed reputation has been used in both MANETs and P2P environments. CORE "Collaborative REputation" mechanism in MANET [6] proposed a watchdog for monitoring and isolating selfish nodes based on a subjective, indirect and functional reputation. CONFIDENT [7] proposed using an adaptive Bayesian reputation and trust system where nodes monitor their neighborhood and detect several kinds of misbehavior. SCAN [4] proposed a network layer security protocol that relies on collaborative localized voting to convict malicious nodes and using asymmetric cryptography to protect the token of normal nodes. Other researches attempted to provide routing layer solutions to black hole attacks, with techniques to identify and isolate these nodes as in [9] [10]. A lot of emerging research attempt to use social theory to address routing/forwarding in opportunistic networks. We attempt in this paper to analyze the impact of using such social parameters to help building a reputation system in such challenged environments. Marti et al [3] proposed to trace malicious nodes by using watchdog/path rater. In watchdog when a node forwards a packet, the node's watchdog verifies that the next node in the path also forwards the packet by promiscuously listening to the next node's transmissions. If the watchdog finds the next node does not forward the packet during a predefined threshold time, the watchdog will accuse the next node as a malicious node to the source node; The proposal has two shortcomings: 1) to monitor the behavior of nodes two or more hops away, one node has to trust the information from other nodes, which introduces the vulnerability that good nodes may be bypassed by malicious accusation; 2) The *watchdog* cannot differentiate the misbehavior from the ambiguous collisions, receiver collisions, controlled transmission power, collusion, false misbehavior and partial dropping.

3. OUR REPUTATION-BASED SECURITY PROTOCOL

3.1 ARCHITECTRE

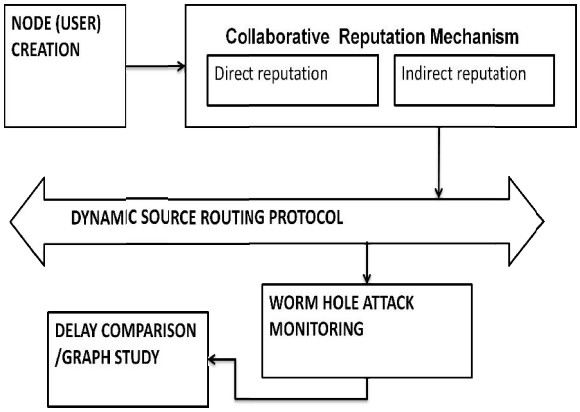

Fig.3.1 Prototype model of reputation based protocol

Our reputation based protocol integrates four main features of distributed reputation systems proposed in [1] and shows how they can be extended by utilizing different kinds of centrality of nodes even in highly mobile and disconnection prone scenarios. Each node in a MANET collects reputation information, through direct observation of its neighbors (subjective observation) and gathers indirect (second hand) reputations from other nods. In addition to using historical observations, our protocol uses reputation discounting to ensure that old reputations will fade away giving more chance for nodes to reclaim their reputation by consistently behaving in a cooperative manner. We use secondary response to retaliate against any neighbor who originally had a bad reputation that then got reclaimed, if this neighbor shows early signs of misbehaver afterwards, to avoid reputation discounting firing back. We employ reputation noise detection and cancellation, deviation test and secondary response that are specifically tailored for our highly challenged environment in order to increase the accuracy and reliability of the reputation resolution.

In this paper we present a mechanism capable of detecting and removing the malicious nodes launching these two types of attacks. In this work, we employ a more aggressive black hole attacks where the malicious node is not only silently dropping the data packets, but also attacking the routing layer. Previous works were only concerned with a passive black hole where the black hole would only drop the traffic that is sent to it as part of the normal topology discovery (no routing malicious behavior). Here in our proposed work we deal with more aggressive routing level attack, in which a black hole would actively reply to topology discovery requests and advertise itself as an attractive route (i.e. advertise itself as having the shortest number of hops to destination, and the highest DSR sequence number than any other RREP to indicate freshness of the route) to any destination(s). This doesn't only cause the malicious nodes to intercept and drop the data packets but also to disrupt communication needed between other good nodes to propagate reputation information necessary for reputation convergence in MANET. Our proposed reputation framework relies on centrality and mobility as two key parameters to drive the system to a more stable state in highly mobile, sparse and disconnected environments.

3.2 DSR (DYNAMIC SOURCE ROUTING)

DSR is a source routing in which the source node starts and take charge of computing the routes. At the time when a node S wants to send messages to node T, it firstly broadcasts a route request (RREQ) which contains the destination and source nodes' identities. Each intermediate node that receives RREQ will add its identity and rebroadcast it until RREQ reaches a node n who knows a route to T or the node T. Then a reply (RREP) will be generated and sent back along the reverse path until S receives RREP. When S sends data packets, it adds the path to the packets' headers and starts a stateless forwarding [9]. During route maintenance, S detects the link failures along the path. If it happens, it repairs the broken links. Otherwise, when the source route is completely broken, S will restart a new discovery.

3.3 THE REPUTATION CONCEPT

In our scheme, MANET nodes can be thought of as members of a community (or subjects) that share a common resource. The key to solve problems related to node misbehavior derives from the strong binding between the utilization of a common resource and the cooperative behavior of the members of the community. Thus, all members of a community that share resources have to contribute to the community life in order to be entitled to use those resources. However, the members of a community are often unrelated to each other and have no information on one another's behavior. We believe that reputation is a good measure of someone's contribution to common network operations. Indeed, reputation is usually defined as the amount of trust inspired by a particular member of a community in a specific setting or domain of interest. Members that have a good reputation, because they helpfully contribute to the community life, can use the resources while members with a bad reputation, because they refused to cooperate, are gradually excluded from the community. The approach presented in this section is used as a basis for the security mechanism that solves the problems due to misbehaving nodes by incorporating a reputation mechanism that provides an automatic method for the social mechanisms of reputation. As an example, disadvantaged nodes that are inherently selfish due to their precarious energy conditions shouldn't be excluded from the network using the same basis as for malicious nodes: this is done with an accurate evaluation of the reputation value that takes into account a sporadic misbehavior.

3.4 PROTOCOL

The CORE scheme involves two types of protocol entities, a requestor and one or more providers, that are within the wireless transmission range of the requestor. The nature of the protocol and the mechanisms on which it relies assure that if a provider refuses to cooperate (i.e. the request is not satisfied), then the CORE scheme will react by decreasing the reputation of the provider, leading to its exclusion if the non-cooperative behavior persists. For sake of simplicity, the following scenarios are related to the execution of the protocol between a requestor and one provider.

3.5 APPLICATION OF CORE TO THE DSR

Route discovery allows any node in the ad hoc network to dynamically discover a route to any node in the ad hoc network, whether directly reachable within wireless transmission range or reachable through one or more intermediate network hops through other nodes. A node initiating a route discovery broadcasts a route *request* message which may be received by those nodes within wireless transmission range of it. When any node receives a route request message it processes the request and if the target of the request is unknown it appends the nodes own address to the route record in the route request packet and re-broadcast the request. If the route discovery is successful the initiating node receives a route *reply* message listing a sequence of network hops through which it may reach the target. As discussed the CORE scheme involves a *requestor* and one or more *providers* that are within the wireless transmission range of the *requestor*. The CORE protocol can be thought of as a layer on top of the DSR protocol, and the function *f* that has to be monitored corresponds to the Route Discovery function of the DSR protocol.

Node misbehavior is detected in the request phase of the Route Discovery function while the reply phase informs the initiator and the intermediate nodes on the identity of the network entities that participated to the Route Discovery phase. Only a cooperative behavior allows an entity to change its reputation value from negative to positive: nodes are stimulated to participate to the Route Discovery function if they want to be served when they need to communicate.

4. OUTPUT OF REPUTATION UPDATES

As a first stage of reputation the keys from every node will be collected and updated. Then MAC address of every node also received separately from every node. Here we consider 20 nodes as the network and start to find the malicious node. Here are the results of the reputation.

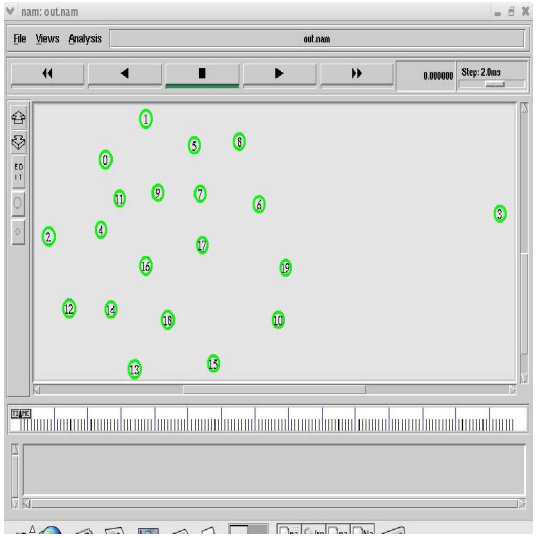

Fig 4.1 Node Creation (20 users)

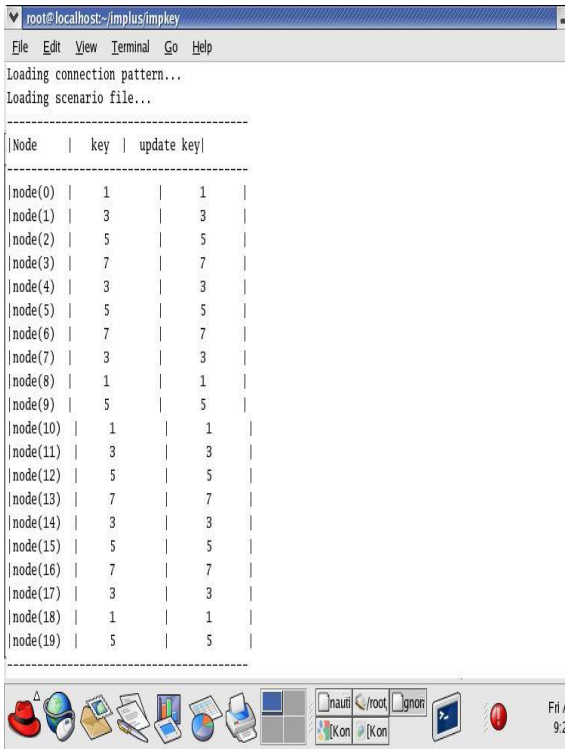

Fig 4.2 Updated keys for every node

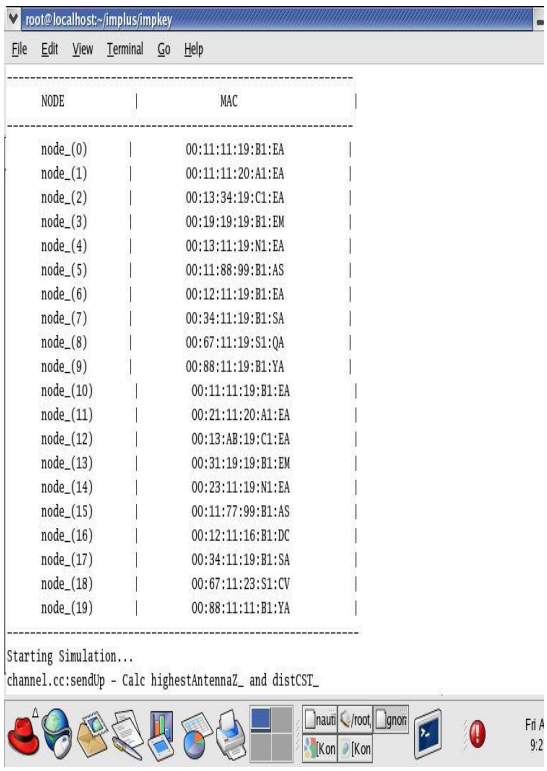

Fig.4.3 MAC address update

5. MALICIOUS NODE DETECTION

Black hole detection is our main concern. Nodes with higher centrality have higher probability of getting in contact with many other nodes than nodes with low centrality. We identify the nodes that have both high centrality and high reputation as preferred sources for indirect reputation. This becomes even more important in high mobility and sparse networks, as nodes often have few connections if any at any point in time, these connections are frequently changing which causes more uncertainty. First we will select four nodes and make them as the server nodes .This is shown in fig.5.1.

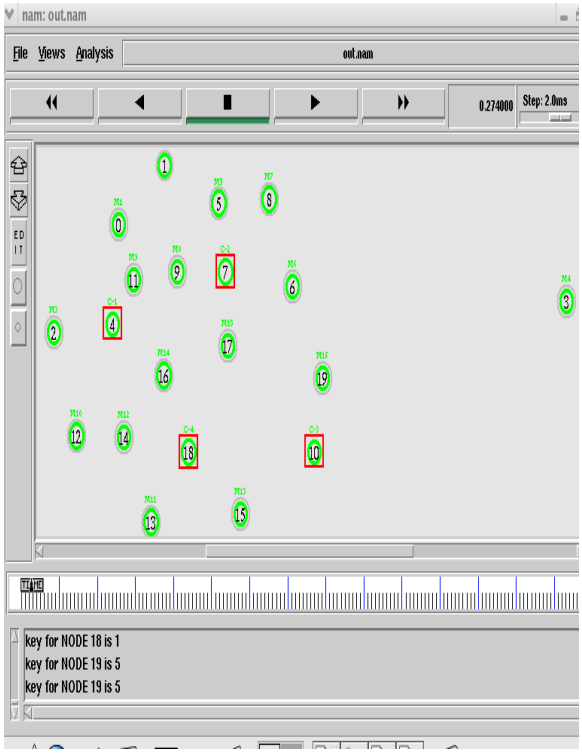

Fig 5.1 Four servers are chosen based on centrality measure.

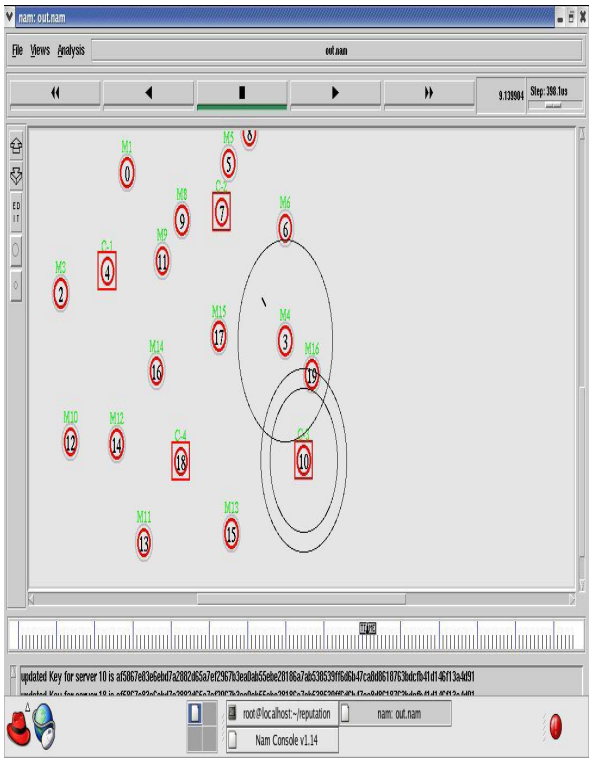

Fig 5.2 Server 10 is sending message to server 7 via node 3

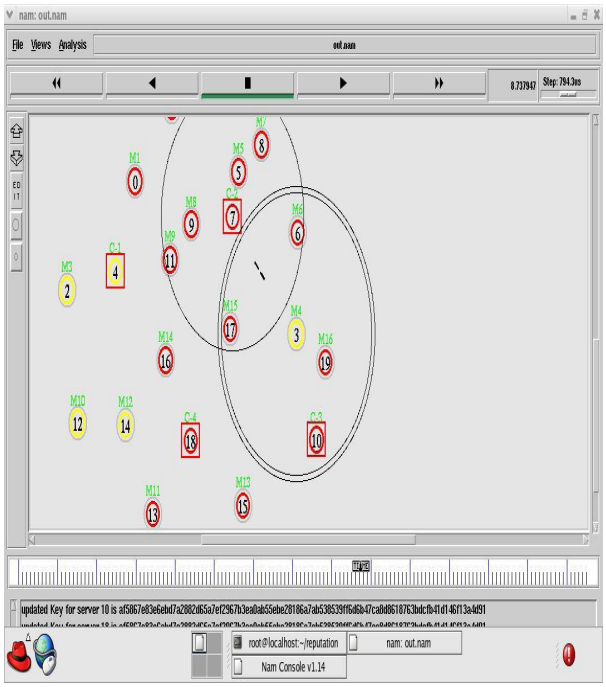

Fig. 5.3 Node 3 is sending the packets to Server 7

Fig 5.4 Node 3 is replying to server 10

Fig 5.5 Node 3 is dropping packets

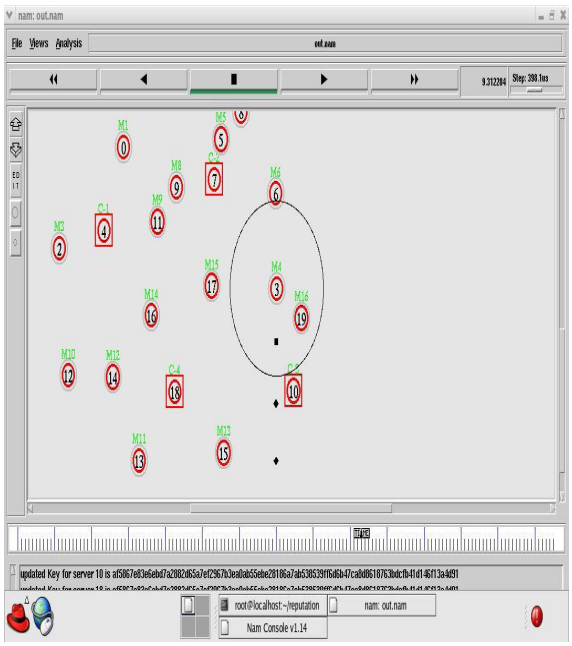

Fig 5.6 Node 3 is dropping packets rapidly (malicious)

Here from the observations it is very clear that for some period of time node 3 is advertising itself as the shortest path and very efficient path and to show that, it is not a malicious node it is acknowledging the node 10. But after some time the packets are dropped by the node 3 this is called black hole attack.

6. CONCLUSION

We have considered the problem of black hole attacks in MANETS and proposed our reputation based protocol for security in MANETS. Our results confirm that active black hole attacks can be detected easily and efficiently than the AODV based reputation protocol.

6.1 Future work

In future with the help of this reputation based routing protocol we will try to resolve the black hole attacks. Delay, jitter and throughput will be compared with the existing AODV based routing protocol.

ACKNOWLEDGEMENT

The authors wish to thank almighty GOD for his grace and the editorial team of IJSER for encouraging our work.

7. REFERENCES

[1] Baruch Awerbuch, Reza Curtmola, David Holmer, Cristina Nita-Rotaru, Herbert Rubens "Mitigating Byzantine Attacks in Ad Hoc Wireless Networks", ACM MobiCom, Aug-2000.

[2] Charles E.Perkins and Elizabeth M. Royer, "Ad hoc on demand distance vector (AODV) routing (Internet-Draft)", Aug- 1998.

[3] Sonja Buchegger and Jean-Yves Le Boudec. Performance Analysis of the CONFIDANT Protocol: Cooperation of Nodes — Fairness In Dynamic Adhoc Networks. In Proc. of IEEE/ACM MobiHOC, 2002. IEEE.

[4] H. Yang, et al, "SCAN: Self-Organized Network-Layer Security in Mobile Ad Hoc Networks," IEEE Network, vol. 24, 2006, pp. 1-13.

[5] P. Michiardi and R. Molva, "CORE: A Collaborative Reputation Mechanism to enforce node cooperation in Mobile Ad hoc Networks", Proc. IFIP CMS, 2002.

[6] S. Buchegger and J.-Y. Le Boudec, "A Robust Reputation System for P2P and Mobile Ad-hoc Networks," Proc. 2nd Workshop Economics of Peer-to- Peer Systems, 2004