International Journal of Computer Science and Engineering (IJCSE)
ISSN: 2278-9960
Vol.1, Issue 2 Nov 2012 11-18

International Academy of Science, Engineering and Technology
Connecting Researchers; Nurturing Innovations

REPUTATION BASED SCHEME FOR ROUTING PROTOCOLS TO HANDLE THE SECURITY ISSUES IN MANETs

[1]GEETHA.V & [2]S.A.HARIPRASAD

[1]Asst. Professor, Dept of ISE, RV College of Engineering, Bangalore-560059, India

[2] Assoc .Professor, Dept of E&C, RV College of Engineering, Bangalore-560059, India

ABSTRACT

In the field of mobile ad hoc networks routing protocols, there are lot of problems to be tackled such as Quality of service, power awareness, routing optimization and security issues. In the proposed work, the main interest is in the security issues related to routing protocols in MANETs. Different existing routing protocols can use the reputation based scheme to improve the security issues. Then more interest in secure routing protocols and their different mechanism in defending against the malicious, compromised and selfish nodes in the mobile ad hoc network is presented. All the secure routing protocols do not account for selfish nodes whether by detecting or isolating them from the network. Therefore, the discusses how to make the Authenticated Routing for Ad Hoc Networks secure routing protocol capable of defending itself against authenticated selfish nodes participating in the mobile ad hoc network. In the upcoming paper, a discussion of a novel conjectural-based scheme to detect and defend against authenticated selfish nodes' attacks in MANETs built upon the routing protocol is presented.

KEYWORDS: Reputation Systems, Routing Protocols, Manets

INTRODUCTION

As nodes in mobile ad hoc networks have a limited transmission range, they expect their neighbors to relay packets meant for far off destinations. These networks are based on the fundamental assumption that if a node promises to relay a packet, it will relay it and will not cheat. This assumption becomes invalid when the nodes in the network have tangential or contradictory goals. The reputations of the nodes, based on their past history of relaying packets, can be used by their neighbors to ensure that the packet will be relayed by the node. In the upcoming subsections, a discussion of a simple reputation-based scheme to detect and defend against authenticated selfish nodes' attacks in MANETs built upon any routing protocol is presented. Sometimes authenticated nodes are congested and they cannot fulfill all control packets broadcasted in the MANET so they choose not to reply to other requests in order to do their own assigned load according to their battery, performance and congestion status. By considering the reputation value of the node asking others to forward its packets. If the packet has originated from a low-reputed node, the packet is put back at the end of the queue of the current node and if the packet has originated from a high-reputed node, the current node sends the data packet to the next hop in the route as soon as possible. This scheme helps in encouraging the nodes to participate and cooperate in the ad hoc network effectively. Authenticated nodes promise to route data packets by replying to control packets showing their interest in cooperation in forwarding these data packets but then they become selfish and start dropping the data packets. This is done by giving incentives to the participating nodes for their cooperation.In this paper the different reputation-based schemes like Confidant and Core, ocean are discussed. Each node keeps only the reputation values of all direct nodes it dealt with. These reputation values are based on the node's first hand experience with other nodes.

REPUTATION-BASED SCHEMES

Reputation systems are applied to wireless mobile ad hoc network to address threats arising from uncooperative nodes. They rely on neighbor monitoring to mitigate selfishness and stimulate cooperation in mobile ad hoc network. In the following subsections, a discussion of the following reputation systems: Confidant, Core and Ocean is given.

Confidant

Buchegger and Boudec presented a reputation-based protocol called Confidant for making misbehavior unattractive. Confidant stands for Cooperation of Nodes: Fairness in Dynamic Ad-hoc Network, it works as an extension to the Dynamic Source Routing (DSR) on demand routing protocol.

Confidant aims at detecting and isolating uncooperative nodes so that to make it unattractive for nodes to deny cooperation. Nodes rely on passive observation of all packets within a one-hop neighborhood. With Confidant, each node has the following four components: a monitor, a trust manager, a reputation system and a path manager. These components interact with each other to provide and process protocol information.

1. The monitor is the equivalent of a neighbor watch, where nodes locally monitor deviating behavior. A node can detect deviation by its neighbor on the source route by listening to the transmission of its neighbor. The monitor reports any suspicious events and any incoming ALARM messages to the trust manager.
2. The trust manager makes decisions about providing or accepting route information, accepting a node as part of a route, or taking part in a route originated by another node. It consists of the following components:
3. An alarm table containing information about received alarms.
4. A trust table managing trust levels for nodes to determine the trustworthiness of an alarm.
5. A friends list containing all the friends that the node may sends alarms to.

ALARM messages containing the type and frequency of protocol violations are sent by the trust manager of a node to warn others of malicious nodes. Outgoing ALARM messages are generated by the node itself after having experienced, observed, or received a report of malicious behavior. The recipients of these ALARM messages are so-called friends, which are administered in a friends list. The source of any Incoming ALARM messages, originated from either outside friends or other nodes, has to be checked for trustworthiness before triggering a reaction.

1. The reputation system in this protocol manages a table consisting of entries for nodes and their rating. The rating is changed only when there is sufficient evidence of malicious behavior that is significant for a node and that has occurred a number of times exceeding a threshold to rule out coincidences. To avoid a centralized rating, local rating lists and/or black-lists are maintained at each node and potentially exchanged with friends.
2. The path manager performs the following functions: path re-ranking according to reputation of the nodes in the path; deletion of paths containing malicious nodes, action on receiving a request for a route from a malicious node and action on receiving request for a route containing a malicious node in the source route.

Each node monitors the behavior of its neighbors. If a suspicious event is detected, the information is given to the reputation system. If the event is significant for the node, it is checked whether the event has occurred more than a predefined threshold that is high enough to distinguish deliberate malicious behavior from simple coincidences such as collisions. If a certain threshold is exceeded, the reputation system updates the rating of the node that caused the event. If

the rating turns out to be intolerable, the information is relayed to the path manager, which proceeds to delete all routes containing the misbehaving node from the path cache.

Core

A mechanism called Core (COllaborative REputation mechanism), was propose to enforce node cooperation in mobile ad hoc network. It is a generic mechanism that can be integrated with any network function like packet forwarding, route discovery, network management and location management and is mainly an extension to the DSR on demand routing protocol.

Core stimulates node cooperation by using a collaborative monitoring technique and a reputation mechanism. In this mechanism, reputation is a measure of someone's contribution to network operations. Members that have a good reputation can use the resources while members with a bad reputation, because they refused to cooperate, are gradually excluded from the community.

This reputation system defines three types of reputation :

1. Subjective reputation is a reputation value which is locally calculated based on direct observation. For example, node X calculates the reputation of a neighbor node Y at a given time for a particular function.
2. Indirect reputation is second hand reputation information which is established by other nodes. For example, node X will accept the indirect reputation of node Y from node Z. To eliminate an attack where a malicious node disseminates false negative reputation information, only positive reputation information is distributed in Core.
3. Functional reputation is related to a certain function, where each function is given a weight as to its importance. For example, data packet forwarding may be deemed to be more important than forwarding packets with route information, so data packet forwarding will be given greater weight in the reputation calculations.

Each node computes a reputation value for every neighbor using a sophisticated reputation mechanism that differentiates between subjective reputation, indirect reputation and functional reputation.

Core consists of two basic components:

- The watchdog mechanism is used to detect misbehavior nodes. When a node forwards a packet, the node's watchdog verifies that the next node in the path also forwards the packet. The watchdog does this by listening promiscuously to the next node's transmissions. If the next node does not forward the packet, then it is considered as misbehaving .
- The reputation table is a data structure stored in each node. Each row of the table consists of four entries: the unique identifier of the entity, a collection of recent subjective observations made on that entity's behavior, a list of the recent indirect reputation values provided by other entities and the value of the reputation evaluated for a predefined function

Ocean

S. Bansal et al. proposed an Observation-based Cooperation Enforcement in Ad hoc Networks (Ocean). In contrast to Confidant and Core, Ocean avoids indirect (second hand) reputation information and uses only direct first hand

observations of other nodes behavior. A node makes routing decisions based solely on direct observations of its neighboring nodes interaction.

In Ocean, the rating of each node is initialized to Neutral (0), with every positive action resulting in an increment (+1) of the rating, and every negative action resulting in a decrement (-2) of the rating. Once the rating of a node falls below a certain faulty threshold (-40), the node is added to a faulty list. The faulty list represents a list of misbehaving nodes. Ocean has five components reside in each node to detect and mitigate misbehavior:

1. NeighborWatch observes the behavior of the neighbors of a node. It works the same way as watchdog. Whenever misbehavior is detected, NeighborWatch reports to the RouteRanker, which maintains ratings of the neighbor nodes.
2. RouteRanker maintains a rating for each of its neighboring nodes. The rating is initialized to Neutral and is incremented and decremented based on observed events from the NeighborWatch component.
3. Rank-Based Routing uses the information from NeighborWatch to make the decision of selection of routes. An additional field, called the avoid-list, is added to the DSR Route-Request Packet (RREQ) to avoid routes containing nodes in the faulty list.
4. Malicious Traffic Rejection rejects traffic from nodes which is considered misbehaving. All traffic from a misbehaving node is rejected so that a node is not able to relay its own traffic under the guise of forwarding it on.
5. Second Chance Mechanism allows nodes previously considered misbehaving to become useful again. A timeout approach is used where a misbehaving node is removed from the faulty list after a fixed period of inactivity. Even though the node is removed from the faulty list, its rating is not increased so that it can quickly be added back to the faulty list if it continues the misbehavior.

Ocean focuses on the robustness of packet forwarding: maintaining the overall packet throughput of mobile an ad hoc network with the existence of misbehaving nodes at the routing layer. Ocean's approach is to disallow any second hand reputation exchanges. Routing decisions are made based solely on direct observations of neighboring nodes' behavior. This eliminates most trust management complexity. Last but not least, Ocean reputation system is mainly an extension to the DSR on demand routing protocol

DESIGN REQUIREMENTS

The following requirements are set while designing the reputation-based scheme to be integrated with any rouitng protocol:

a. The reputation information should be easy to use and the nodes should be able to ascertain the best available nodes for routing without requiring human intervention.

b. The system should not have a low performance cost because low routing efficiency can drastically affect the efficiency of the applications running on the ad hoc network.

c. Nodes should be able to punish other selfish nodes in the MANET by providing them with a bad reputation.

d. The system should be built so that there is an injection of motivation to encourage cooperation among nodes.

e. The collection and storage of nodes' reputation values are done in a decentralized way.

f. The system must succeed in increasing the average throughput of the mobile ad hoc network or at least maintain it.

The proposed protocol will be structured into the following four main phases. which will be explained in the subsequent subsections:

- Route Lookup Phase
- Data Transfer Phase
- Reputation Phase
- Timeout Phase

Route Lookup Phase

This phase mainly incorporates the authenticated route discovery and route setup phases of the normal secure routing protocol. In this phase, if a source node S has packets for the destination node D, the source node broadcasts a route discovery packet (RDP) for a route from node S to node D. Each intermediate node interested in cooperating to route this control packet broadcasts it throughout the mobile ad hoc network; in addition, each intermediate node inserts a record of the source, nonce, destination and previous-hop of this packet in its routing records. This process continues until this RDP packet reaches the destination. Then the destination unicasts a route reply packet (RREP) for each RDP packet it receives back using the reverse-path. Each intermediate node receiving this RREP updates its routing table for the next-hop of the route reply packet and then unicasts this RREP in the reverse-path using the earlier-stored previous-hop node information. This process repeats until the RREP packet reaches the source node S. Finally, the source node S inserts a record for the destination node D in its routing table for each received RREP.

In the below figures, the route lookup phase is presented in details, illustrating the two phases of it, the authenticated route discovery phase and the authenticated route setup phase.

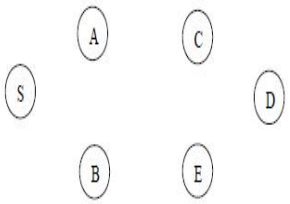

Fig. 1: MANET Environment

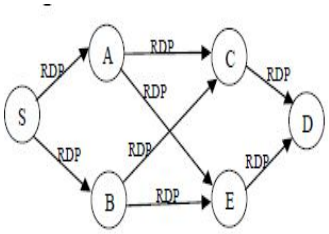

Fig. 2: Broadcasting RDP

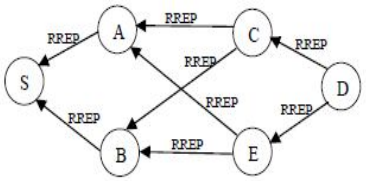

Fig. 3: Replying to Each RDP

Data Transfer Phase

At this time, the source node S and the other intermediate nodes have many RREPs for the same RDP packet sent earlier. So, the source node S chooses the highly-reputed next-hop node for its data transfer. If two next-hop nodes have the same reputation, S will choose one of them randomly, stores its information in the sent-table as the path for its data transfer. Also, the source node will start a timer before it should receive a data acknowledgement (DACK) from the destination for this data packet. Afterwards, the chosen next-hop node will again choose the highly-reputed next-hop node from its routing table and will store its information in its sent-table as the path of this data transfer. Also, this chosen node will start a timer, before which it should receive the DACK from the destination for this data packet. This process continues till the data packet reaches the destination node D. And of course in this phase, if the data packet has originated from a low-reputed node, the packet is put back at the end of the queue of the current node. If the packet has originated from a high-reputed node, the current node sends the data packet to the next highly-reputed hop in the route discovered in the previous phase as soon as possible. Once the packet reaches its destination, the destination node D sends a signed data acknowledgement packet to the source S. The DACK traverses the same route as the data packet, but in the reverse direction. In the following figures, the data transfer phase is illustrated:

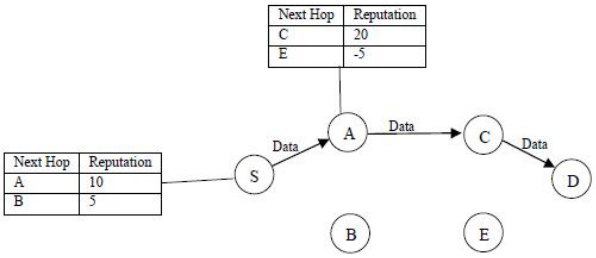

Fig. 4: Choosing the Highly Reputed Next Hop Node

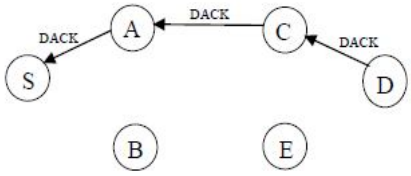

Fig. 5: Sending DACK for Each Received Data Packet

Reputation Phase

In this phase, when an intermediate node receives a data acknowledgement packet (DACK), it retrieves the record, inserted in the data transfer phase, corresponding to this data packet then it increments the reputation of the next hop node. In addition, it deletes this data packet entry from its sent-table. Once the DACK packet reaches node S, it deletes this entry from its sent-table and gives a recommendation of (+1) to the node that delivered the acknowledgement.

Timeout Phase

In this phase, once the timer for a given data packet expires at a node, the node retrieves the entry corresponding to this data transfer operation returned by the timer from its sent-table. Then, the node gives a negative recommendation (-2) to the next-hop node and deletes the entry from the sent-table. Later on, when the intermediate nodes' timers up to the node that dropped the packet expire, they give a negative recommendation to their next hop node and delete the entry from their sent-table. As a consequence, all the nodes between the selfish node and the sender, including the selfish node, get a recommendation of (-2). Now, if the reputation of the next-hop node goes below the threshold (-40), the current node deactivates this node in its routing table and sends an error message RERR to the upstream nodes in the route. Now, it is the responsibility of the sender to reinitiate the route discovery again. In addition, the node whose reputation value reached (-40) is now temporally weeded out of the MANET for five minutes and it later joins the network with a value of (0) so that to treat it as a newly joined node in the network.

ANALYSIS OF THE PROPOSED REPUTED-SECURE ROUTING PROTOCOL

In this section, an analysis of the proposed reputation-based scheme is given by discussing different authenticated selfish nodes' forms of attacks and presenting ways of counteracting them by the introduced reputation-based scheme.

- An authenticated selfish node might make a false claim of knowing the route to a destination and generate a RREP for a destination for which it does not have a route. This attack can be foiled by the proposed reputation-based scheme routing. After receiving the data packet for the corresponding destination, this authenticated selfish node will have to drop the data packet. The sender and the intermediate nodes until this selfish node will give a negative recommendation to it. Thus, once the reputation of this selfish node falls below the threshold reputation, it will be considered as selfish and will eventually be temporary ostracized.
- An authenticated selfish node might not reveal that it knows the route to the destination by not replying to or forwarding control packets so that to save its resources, such as energy and processing power; by doing this selfish behavior, it will not be able to inflict any damage to the network as it will not be able to drop the data packets routed via other paths. To face this type of selfish attack, the proposed scheme considers the reputation value of the node asking others to forward its packets. If the packet has originated from a low-reputed node, the packet is assigned lowermost priority and if the packet has originated from a high-reputed node, the current node sends the data packet to the next hop in the route as soon as possible. Hence, these selfish nodes will see a considerable increase in network latency. So, the proposed scheme helps in encouraging the nodes to participate and cooperate in the ad hoc network effectively.
- An authenticated selfish node might promise to route data packets, but then it starts to drop all the data packets that it receives. The presented reputation-based scheme foils this attack. In such a scenario, the upstream neighbor of the node will give it a negative recommendation and the reputation of the node will be reduced. Eventually, the node will be weeded out of the network for a period of time.
- Authenticated selfish nodes might collude by giving positive recommendations to each other so that to increase their reputations. The proposed reputation-based scheme prevents this attack by having the nodes rely on their own experience rather than the experience of their peers. Although the exchange of reputation information among the nodes will make the system more robust, it is not incorporated in my scheme. This is due to that if the nodes exchange the reputations of other nodes, the target (node soliciting reputation of another node) will have to consider the credibility of the information source (node providing reputation of another node). As a result, this

will imply more work for the nodes at the routing layer and will also increase the volume of the network traffic [20]. The downside of my scheme is that an authenticated selfish node can move around the network and selectively drop packets from different neighbors without getting caught for a long time. However, eventually this selfish node will be caught.

- An authenticated selfish node might continuously drops data packets to decrease the throughput of the mobile ad hoc network. The presented scheme can prevent such attack. Since the nodes in an ad hoc network are semi-autonomous, the proposed reputation-based scheme motivates them to allocate their resources to other nodes in the network. As the sender relays the packet only to highly reputed neighbors, it reduces the risk that its neighbors will intentionally drop the packet. The neighbors in turn forward the packets to nodes that have a high reputation with them. As a result, the number of packets intentionally dropped is reduced and the throughput of the system rises.
- An authenticated well-behaved node might become a bottleneck since in the presented reputation-based scheme the node with the highest reputation is selected as the next hop by its neighbor. As a result, the nodes with higher reputations will become overloaded, while the other nodes become totally free . This problem is prevented in the proposed scheme as when authenticated nodes are congested and they can not fulfill all control packets broadcasted in the MANET, they can choose not to reply to other nodes' requests in order to do their own assigned load according to their battery, performance and congestion status.

SUMMARY

The field of ad hoc mobile networks is rapidly growing and changing, and while there are still many challenges that need to be met, it is likely that such networks will see widespread use within the next few years. In this chapter, a new reputation-based scheme to be integrated with one of the secure routing MANET protocols, Any routing protocol to make it detect and defend against selfish nodes and their misbehavior is presented. An explanation of the different phases of this scheme and analysis of the various forms of selfish attacks that this scheme defends against are presented.

REFERENCES

1. A. Sun, The design and implementation of fisheye routing protocol for mobile ad hoc networks. M.S. Thesis, Department of Electrical and Computer Science, MIT, May 2002.
2. R. Duggirala. A Novel Route Maintenance Technique for Ad Hoc Routing Protocols. M.S. Thesis, University of Cincinnati, November 2000.
3. abdahalla mohamed. Reuted – ARAN, M.S. Thesis, American University in cairo, May 2005.
4. P. Dewan and P. Dasgupta. Trusting Routers and Relays in Ad hoc Networks. First International Workshop on Wireless Security and Privacy in conjunction with IEEE International Conference on Parallel Processing Workshops (ICPP), October2003.
5. P. Yau and C. Mitchell. Reputation methods for routing security for mobile ad hoc networks. Proceedings of SympoTIC, Joint IST Workshop on Mobile Future and Symposium on Trends in Communications, October 2003, pages 130-137.