Authenticated Routing Protocol Based on Reputation System For Adhoc Networks

Preeti Nagrath
BharatiVidyaPeeth College of Engg.
Delhi, India

Ashish kumar
BharatiVidyapeeth College of Engg.
Delhi, India

Shikha Bhardwaj
BharatiVidyaPeeth College of Engg.
Delhi, India

***Abstract*-Dynamic nature of adhoc networks leads to challenges in securing the network. Due to vulnerable nature of adhoc networks there are many security threats. Much work is going on to provide security to the network. One of the solution to the problem is ARAN – Authenticated routing protocol which is a secure protocol and provides Integrity, Availability, Confidentiality, Authenticity, Non repudiation, Authorization & Anonymity but an authenticated selfish node can infer to this protocol performance and can disturb the network by dropping packets. This paper discusses reputation based schemes that can be applied to ARAN to detect selfish node and improve the performance.**

***Keywords*:--**Selfish node, RDP, RREP, DACK, Malacious node, Reputation based Schema

1. INTRODUCTION

A Mobile Adhoc Network (MANET) have a set of mobile hosts to carry out various networking functions like packet forwarding, routing and service discovery without the help of any pre deployed infrastructure. These nodes self organize without central management. Nodes move freely resulting in changes to the network topology and updated routing in order to forward the packets. Due to dynamic nature of adhoc network securing the network is a big challenge. Many routing protocols have been proposed like AODV, DSR to handle the network with large number of hosts with limited resources like energy and bandwidth but no security consideration have been made, and then many secure routing protocols are developed to secure the network. Security implies identification of threats, attacks and vulnerability in the network. ARAN – authenticated routing protocol is a secure protocol which provides security for attacks using modification, fabrication, impersonation and securing shortest paths [3]. It was proposed by Sanzgiri, Laflamme, Dahill, Levine, Shields and Belding, Royer [1]. It is based on adhoc on demand distance vector routing so as to take benefit of high performance and low cost due to it's on reactive nature. It detects and protects against malicious activities caused by other nodes and peers. ARAN introduces Authentication, message repudiation to an adhoc environment as a part of minimal security policy [1].

This paper is organized as follows:

Section 2 presents analysis of ARAN & then it discusses the problem of Selfish node in ARAN.

Section 3 presents various schemes for stimulating co-operation among such selfish nodes & to ensure optimum network utilization.

Section 4 presents Reputation Based Schema for ARAN.

Section 5 offers conclusion and future work.

2.The most common Routing protocol AODV handles the dynamic and rapidly changing Adhoc Network very efficiently but not securely .From the view point of security every protocol must satisfy the following criteria[3]

Certain Discovery, Isolation, Light weight Computation, Byzantine Robustness.

There are certain exploits which are allowed by the existing protocols like AODV & DSR are Attacks using Modification[1],which includes Redirection by modified route sequence numbers, Redirection with modified hop counts, Denial of Service with modified source routes & Tunneling .Attacks using Fabrication includes falsifying Route Errors, Route Cache poisoning.

There are two types of Adhoc Network nodes:

a.Malacious Nodes-These are the nodes that suppress the correct function of routing protocol by modifying routing information, fabrication false information. It is the node that aims at damaging other nodes by causing network outage by partitioning while saving battery life is not a priority[4].Malicious network nodes that participate in routing protocols but refuse to forward protocols but refuse to forward messages may corrupt a MANET.

B.Selfish Nodes-These nodes severely degrade network performance and eventually partition the network by simply not participating in the network operation. [14].

ARAN Security Analysis:-ARAN[1] makes use of cryptographic certificates to offer routing security and to accomplish its task with authencity .its main feature is to find & protect from misbehaving nodes from third party .For using Aran one has to pay less performance cost to achieve high security .

Solution to vulnerabilities by ARAN:

1. Unauthorized Participation: Without authorization from trusted certificate server, no node can work, so there is no chance of unauthorized participation.

2. Attacks against Fabrication: ARAN ensures Non-Repudiation & prevents spoofing & Un authorization participation in routing.

3. Attacks against Impersonation: Route Discovery Packets (RDP) [3] contains the difference of source node and is signed with source's private key. Similarly, Reply Packets (RREP) includes Destination Node's Certificate& Signature which ensures that destination can respond to Route

Discovery. This prevents Impersonation Attacks where either the source or destination node is Spoofed [2].
4. No Alternation of Routing Messages: As we know that all fields of RDP & RREP packets are specified in ARAN & they remain unchanged between Source and Destination [2].Hence Modification Attacks can be prevented.
5. Attacks Using Modification of Protocol Message: The initiating node signs both packet types, any alternation would be detected & the altered packet would be thrown out.
6. Denail of Service Attacks: can be conducted by nodes with or without valid ARAN Certificates:
A. in Certificate less case: All possible Attacks are limited to the attackers' immediate neighbors because unsigned route requests are dropped.
B.In Certificate case: Nodes with valid certificated can conduct effective Denial of Service attacks by sending unnecessary route requests & they will go undetected as the current existing RAN protocol cannot differentiate between legitimate & malicious RREQ's coming from authenticated nodes [3].

3.SELFISH NODE WEAKNESS OF ARAN:-An individual mobile node may attempt to benefit from other nodes but denies to share its own resources .These are known as Selfish Nodes and this behavior is termed as Selfishness. This un co-operative behavior can lead to breakdown of whole communication network.

ARAN is capable of defending itself against Spoofing, Fabrication, Modification, and DOS Attacks. The currently existing ARAN secure protocol does not account for attacks conducted by Authenticated Selfish Nodes as these nodes trust each other to co operate in providing network functionalities. So ARAN is not capable to detect & defend against selfish node. If un authenticated Selfish node does not forward or intentionally drop control or data packets ,the current specification of ARAN cannot detect Selfish nodes .This weakness of ARAN can cause disturbance in MANETS & leads to wastage of network bandwidth.
Techniques to detect Selfish Nodes:
Various techniques have been proposed to detect and prevent Selfish Nodes in Manets. Nodes may exhibit non, cooperation by refusing to route packets due to several reasons such as power and other resource constraints or intent to deliberately disrupt the system. There are various approaches for stimulating co-operation .These approaches are mostly
a. Incentive based /Credit based /Virtual Currency Based Schemes
B.Punishment based /Reputation Based Schemes [14].

Incentive based schemes are normally implemented using credits that are given to nodes that co-operate & forward packets. The basic problem with these schemes is they either depend on use of temper proof hardware to monitor the increase or decrease of virtual currency or require a central server to determine the change and credit to each node involved in the transmission of a message. However these approaches suffer from location privilege problem [8].

Punishment based schemes identify & punish nodes that exhibit non co-operative behavior. These schemes define a metric called Reputation, in which is the goodness of a Node, as perceived by the neighbors & the reputation is decreased on evidence of non co-operation, so these are called Reputation based Schema. These Schemes are based on observation & tests .Nodes which is detected doing misbehavior is informed to other nodes in order to exclude the suspicious node from the Network. The main function of Reputation Based Schemes is Monitoring, Reputation and Response. Based on these functions the reputation based scheme aims at detecting selfish behavior on packet forwarding when it appears in the network.
In [15], Marti et al, proposed a scheme that contains two major modules, termed as Watchdog and Path rater to detect & mitigate respectively. Due to its reliance on overhearing, however the Watchdog technique may fail to detect misbehavior or raise false alarms in the presence of ambiguous collisions & limited transmission power.
The CONFIDANT protocol proposed by Buchegger & le Boudec on [13] is based on selective altruism & utilitarianism, this making misbehavior unattractive. It has four components-Monitor, The Reputation System, The Path Manager & the Trust Manager. The monitor component of CONFIDANT Scheme observes the next hop neighbors behavior using the over hearing technique .This scheme causes same problems as the Watchdog Scheme.
S.Bansal et al, proposed an observation based Co-Operation enforcement in Adhoc Networks (OCEAN) [16].In contrast to CONFIDANT, OCEAN avoids in direct (second hand) reputation information & uses only direct first hand observation of other nodes behavior .A Node makes routing decisions only on the basis of direct observation. In this scheme, Rating is given to each node; initially each node is given value Null (0) - Neutral. With every positive action its value is incremented by 1 & with every negative action its value is decremented by 2.If the rating of node falls below a certain faulty threshold (-40).it is added to the list of faulty nodes.

4. THE PROPOSED REPUTATION BASED SCHEMA: REPUTED-ARAN

There are two attacks which an authenticated selfish node can perform that the current ARAN protocol cannot defend against. To illustrate these two possible attacks that a selfish node can use to save its resources in a MANET communication, the attack-tree notation proposed by Bruce Schneier [19] that allows the categorization of attacks that lead an attacker to reach a specific goal is used. In the below table, the attack tree that cannot be detected by current ARAN protocol is shown:

Attack tree: Save own resources
OR 1. Do not participate in routing
1. Do not relay routing data
OR 1. Do not relay route requests
2. Do not relay route replies
2. Do not relay data packets
1. Drop data packets

Attack Tree: Save own Resources [19]

when nodes simply drop packets (case 1.1 and 2.1 in the attack tree), all the security features of ARAN fail to detect or defend against these attacks, as they focus only on the detection of malicious nodes' attacks and not the

authenticated selfish nodes' attacks. The scheme is used to detect the selfish nodes –which start dropping the packets. This is done by giving incentives to the participating nodes for their cooperation. The proposed scheme is called Reputed-ARAN. Different from global indirect reputation-based schemes like Confidant and Core, the proposed solution uses local direct reputations only like in Ocean reputation-based scheme. Each node keeps only the reputation values of all direct nodes it dealt with. These reputation values are based on the node's firsthand experience with other nodes.

In the proposed reputation scheme, all the nodes in the mobile ad hoc network are assigned an initial value of null (0) as in the Ocean reputation-based scheme [16]. Also, the functionality of the normal ARAN routing protocol in the authenticated route setup phase is modified so that instead of the destination unicasts a RREP to the first received RDP packet of a specific sender only, the destination will unicast a RREP for each RDP packet it receives and forward this RREP on the reverse-path. The next-hop node will relay this RREP. This process continues until the RREP reaches the sender. After that, the source node sends the data packet to the node with the highest reputation. Then the intermediate node forwards the data packet to the next hop with the highest reputation and the process is repeated till the packet reaches its destination. The destination acknowledges the data packet (DACK) to the source that updates its reputation table by giving a recommendation of (+1) to the first hop of the reverse path. All the intermediate nodes in the route give a recommendation of (+1) to their respective next hop in the route and update their local reputation tables. If there is a selfish node in the route, the data packet does not reach its destination. As a result, the source does not receive any DACK for the data packet in appropriate time. So, the source gives a recommendation of (-2) to the first hop on the route. The intermediate nodes also give a recommendation (-2) to their next hop in the route up to the node that dropped the packet. As a consequence, all the nodes between the selfish node and the sender, including the selfish node, get a recommendation of (-2). The idea of giving (-2) to selfish nodes per each data packet dropping is due to the fact that negative behavior should be given greater weight than positive behavior. In addition, this way prevents a selfish node from dropping alternate packets in order to keep its reputation constant. This makes it more difficult for a selfish node to build up a good reputation to attack for a sustained period of time [19]. Moreover, the selfish node will be isolated when its reputation reaches a threshold of (-40) as in the Ocean reputation-based scheme [16]. In the following table, the default Reputed-ARAN parameters are listed:

Initial Reputation	0
Positive Recommendation	+1
Negative Recommendation	-2
Selfish drop Threshold	-40
Re-induction timeout	5 minutes

The proposed protocol is structured into the following four main phases [42] as:

- 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 ARAN secure routing protocol. In this phase, if a source node S has packets for the destination node X, the source node broadcasts a route discovery packet (RDP) for a route from node S to node X.

S → brdcst:[RDP,IPx,Ns]Ks-,CertS

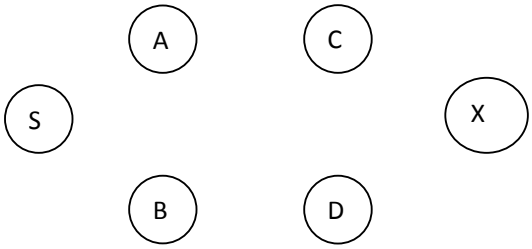
Where IPx is ip address of destination, NS is nonce, KS- is sign of S, CertS is certificate of source S

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. Here KB- is sign of B and CertB is certificate of B.

B → brdcst:[[RDP,IPx,Ns]Ks-]KB-,CertS,CertB

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 X in its routing table for each received RREP

All this can be diagrammatically shown as



As Fig1: A MANET Environment

Let S be the source,

A, B, C, D is the intermediate nodes

X be the destination

When RDP Packet is broadcasted:-

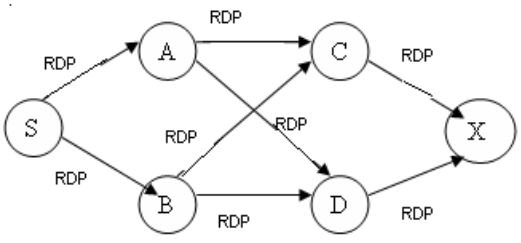


Fig 2: Broadcasting RDP

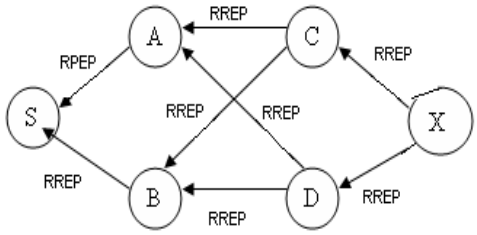


Fig3: Replying to each RDP

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. Afterward 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. This process continues till the data packet reaches the destination node D. 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 as: Here let A Node is having more reputation value than B, So Source S chooses A as next Hop, similarly Node A chooses C node as next Hop if its reputation value comes more than D

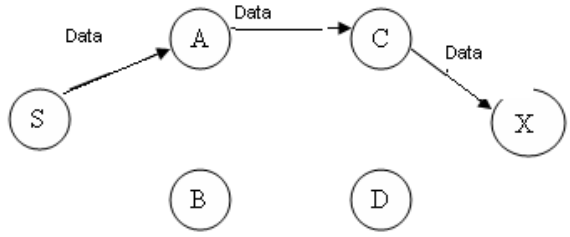


Fig4: Choosing the highly reputed next hop node

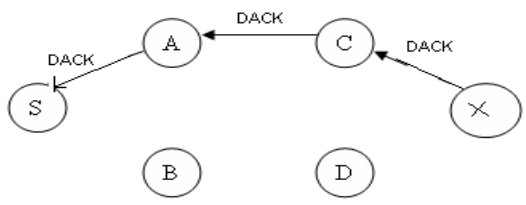


Fig5: Sending data Acknowledgement for each received data packet

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, when 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, 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. Then the original ARAN protocol handles it. 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.

CONCLUSION:-

The field of ad hoc mobile networks is rapidly growing and changing, and while there are still many challenges. In this paper, a reputation-based scheme to be combined with one of the secure routing MANET protocols, ARAN, to make it detect and defend against selfish nodes and their misbehavior. An explanation of the different phases of this scheme and analysis of the various forms of selfish attacks that this scheme defends against are studied. Reputed – ARAN is more efficient and more secure than ARAN secure routing protocol in defending against both malicious and authenticated selfish nodes.

REFERENCES:

[1] K. Sanzgiri, B. Dahill, B.N. Levine, C. Shields, E.M. Belding-Royer, A secure routing protocol for ad hoc networks, in: Proceedings of 2002 IEEE International Conference on Network Protocols (ICNP), November 2002

[2] Mahmoud A,Sameh A,El-Kassas S. Reputed Authenticated Routing for Ad Hoc Networks Protocol(Reputed-ARAN)[A].Proc of the IEEE Int'l Conf on Mobile AdHoc and Sensor Systems[C].2005.787-794.JOURNAL OF COMMUNICATIONS, VOL. 3, NO. 6, NOVEMBER 2008 49© 2008 ACADEMY PUBLISHER

[3] Seema Mehla et. al. / (IJCSE) International Journal on Computer Science and EngineeringVol. 02, No. 03, 2010, 664-668

[4] Selfish nide detection in MANETS by Dr.Janet,P.VIsu,M.Monisha Devi,S.Subhashini

[5] Security issues in MAMETS by Wenjia li and Anupam Joshi

[6] IJCSNS International Journal of ComputerScience and Network Security, VOL.10 No.4,April 2010,Jhaveri et al

[7] Y.-C. Hu, A. Perrig, D.B. Johnson,Wormhole detection in wirelessad hoc networks, A Technical Report TR01-384,Rice UniversityDepartment of Computer Science.

[8] E. Royer and C. Toh. A Review of Current Routing Protocols for Ad Hoc Mobile Wireless Networks. IEEE Personal Communications, April 1999, pages 46-55.

[9] R. Molva and P. Michiardi. Security in Ad hoc Networks. Personal Wireless Communication, September 2003, pages 756-775.

[10] L. Zhou and Z. Haas. Securing Ad Hoc Networks. IEEE Networks Special Issue on Network Security. November/December 1999, pages 24-30.
[11] V. Gayraud and B. Tharon. Securing Wireless Ad Hoc Networks. ISS Master, MP 71 project, March 2003.
[12] P. Michiardi and R. Molva. Simulation-based Analysis of Security Exposures in Mobile Ad Hoc Networks. Proceedings of European Wireless Conference, February 2002.
[13] S. Buchegger and J. Le Boudec. Performance Analysis of the CONFIDANT Protocol: Cooperation of Nodes, Fairness In Dynamic Ad-hoc NeTworks. Proceedings of IEEE/ACM Symposium on Mobile Ad Hoc Networking and Computing, MobiHoc, June 2002.
[14] S. Buchegger and J. Le Boudec. A Robust Reputation System for P2P and Mobile Ad-hoc Networks. Proceedings of the Second Workshop on the Economics of Peer-to-Peer Systems, June 2004.
[15] S. Marti, T. Giuli, K. Lai, and M. Baker. Mitigating routing misbehavior in mobile ad hoc networks. Proceedings of MOBICOM, August 2000.
[16] S. Bansal and M. Baker. Observation-based Cooperation Enforcement in Ad Hoc Networks. http://arxiv.org/pdf/cs.NI/0307012, July 2003.
[17] Mahmoud A,Sameh A,El-Kassas S. ReputedAuthenticated Routing for Ad Hoc Networks ProtocolA Cooperative Secure Routing Protocol based on Reputation System for Ad Hoc Networks JOURNAL OFCOMMUNICATIONS, VOL. 3, NO. 6,NOVEMBER 2008
[18] (Reputed-ARAN)[A].Proc of the IEEE Int'l Conf on Mobile AdHoc and Sensor Systems[C].2005.787-794.JOURNAL OF COMMUNICATIONS, VOL. 3, NO. 6, NOVEMBER 2008 49 © 2008 ACADEMY PUBLISHER
[19] B. Schneier. Attack Trees: Modeling security threats. Dr Dobb's Journal, December 199923. 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.