An On-Demand Byzantine-Resilient Secure Routing Protocol for Wireless Adhoc Networks

Saju P John
Department of Computer Science
Thejus Engineering College
Thrissur , India - 680 584

Philip Samuel
School of Engineering
Cochin University of Science& Technology
India - 682 022

Summary
Security has become a primary concern in order to provide protected communication between mobile nodes in a hostile environment. We refer to any arbitrary action by authenticated nodes resulting in disruption of the routing service such as drop packets, modify packets and miss-route packets as Byzantine behavior, and to such an adversary as a Byzantine adversary. Nodes may exhibit Byzantine behavior, either alone or colluding with other nodes. Several routing protocols were proposed to cope with insider attacks, outsider attacks and selective data forwarding attacks. To mitigate these vulnerabilities of routing protocols in wireless adhoc networks, we propose a new Byzantine-Resilient Secure Routing Protocol (BRSR) that provides resilience against Byzantine attacks. The proposed protocol provides security for inside attacks, outside attacks and selective data forwarding attacks in mobile adhoc networks. Simulation results demonstrate that BRSR effectively mitigates the identified attacks while providing better delivery ratio, and also more resistant against node capture attacks.
Key words:

1. Introduction

Wireless ad-hoc network is a computer network that uses wireless communication links. In wireless adhoc networks each node is willing to forward data for other nodes. This is in contrast to wired network technologies in which the task of forwarding the data is performed using some designated nodes, usually with custom hardware and variously known as routers, switches, hubs, and firewalls. In addition, it is in contrast to managed wireless networks in which a special node known as an access point manages communication among other nodes is used. Mobile ad hoc networks (MANETs), Wireless mesh networks, and wireless sensor networks are the three types of wireless ad-hoc networks. The Ad hoc networks are appropriate for emergency situations like natural disasters or military conflicts due to their minimal configuration and quick deployment. They are appropriate for a variety of applications where central nodes cannot be relied on due to the decentralized nature of most wireless ad hoc networks that in comparison to wireless managed networks improve the scalability of wireless ad-hoc networks.

Routing protocols for ad hoc networks generally can be divided in to two main categories: *periodic* protocols and *on-demand* protocols. In a periodic (or proactive) routing protocol, nodes periodically exchange routing information with other nodes in an attempt to have each node always know a current route to all destinations . In an on-demand (or reactive) protocol, on the other hand, nodes exchange routing information only when needed, with a node attempting to discover a route to some destination only when it has a packet to send to that destination[13].The proposed protocol is an on-demand (reactive) protocol that provides resilience against Byzantine attacks.

1.1 Security Threats in MANET

In order to provide protected communication between mobile nodes in a hostile environment security has become a primary concern [1]. In contrast to the wire line networks, a number of nontrivial challenges are posed to security design by the unique characteristics of mobile ad hoc networks, for instance open peer-to-peer network architecture, shared wireless medium, stringent resource constraints, and highly dynamic network topology. The research activities about security in MANETs are still at their beginning, while the routing aspects of MANETs are already well understood. In addition to the problems of regular networks, a number of new security problems are also faced by MANETs [2].some of the vulnerabilities are as follows.

Due to the very nature of wireless communication, the communication channel is highly insecure. Eavesdropping and masquerading are not very difficult. Node security is another major concern as mobile nodes can fall into hostile control. There have been widely reported cases of theft of cellular nodes, so MANET nodes would not be any safe. The node could be compromised and thus would act as a hostile node. Easy theft might also lead to node tampering. Tampered node might disrupt network operations or release critical information. The limited powers in the

Manuscript received January 5, 2010
Manuscript revised January 20, 2010

mobile nodes can lead to a simple denial of service attack where the attacker could create additional transmissions or expensive computations. The absence of infrastructure stops us from using the classical solutions based on certification authorities and on-line servers. Lack of fixed topology requires the routing protocols to be highly sophisticated. Securing such a protocol in the presence of hostile nodes presents a challenge.

Without appropriate protection, the malicious nodes can readily function as routers and prevent the network from correctly delivering the packets. For example, the malicious nodes can announce incorrect routing updates which are then propagated in the network, or drop all the packets passing through them. Thus security issue in ad hoc networks, namely the protection of their network-layer operations from malicious attacks is very important.

1.2 Security Requirements in Adhoc Networks

All Secure ad hoc routing protocols must satisfy the following requirements to ensure that path discovery from source to destination functions correctly in the presence of malicious adversaries [12]

Route signaling cannot be spoofed; Fabricated routing messages cannot be injected into the network; Routing messages cannot be altered in transit, except according to the normal functionality of the routing protocol; Routing Loops cannot be formed through malicious action; Routes Cannot be redirected from the shortest path by malicious action; Unauthorized nodes should be excluded from route computation and discovery; The network topology must not be exposed neither to adversaries nor to authorized nodes by the routing messages. Exposure of the network Topology may be an advantage for adversaries trying to destroy or capture nodes.

Significant work focused on the security of unicast wireless routing protocols. Several secure routing protocols resilient to outside attacks such as authentication were proposed in the last few years such as Ariadne [8], SEAD [13], and ARAN [12]. Several routing protocols were proposed to cope with insider attacks such as dropping packets, modifying packets [8] – [11]. Methods proposed to address insider threats in routing include monitoring [9], multi-path routing [8], [10] and acknowledgment-based feedback [5].

1.3 Byzantine Attacks

The term “Byzantine behavior” denotes any arbitrary action by authenticated nodes resulting in disruption of the routing service and “Byzantine adversary” denotes such an adversary. Either single nodes or joint nodes may exhibit Byzantine behavior. Not forwarding packets, injecting, modifying or replaying packets, rushing packets or creating wormholes are some examples of such behavior.

- A Byzantine adversary can drop the request and/or response, or can influence the route selection by using wireless specific attacks such as wormhole and flood rushing to prevent a route from being established.
- In addition, the packets carrying the route selection metric such as hop count or node identifiers can be modified by a Byzantine adversary.
- An attacker can inject bogus route activation messages, or drop correct route activation messages to prevent a path from being activated.

We propose a new Byzantine-Resilient Secure Routing Protocol (BRSR) that provides resilience against Byzantine attacks to mitigate these vulnerabilities of routing protocols in wireless ad hoc networks.

2. Related work

A mechanism of detecting node misbehavior in terms of selfishness was presented by Tarag Fahad and Robert Askwith. The working of their algorithm has been illustrated with two scenarios. Their algorithm PCMA detected selfish nodes which perform full/partial packets attack in a successful manner [3].

A credit-based Secure Incentive Protocol (SIP) that simulates cooperation in packet forwarding for infrastructure less MANETs was proposed by Yanchao Zhang. SIP was cautiously designed to be a secure yet lightweight charging and remuneration protocol and to be able to withstand a wide range of cheating actions. In addition, SIP uses a space-efficient Bloom filter that provided low communication overhead [4].

The routing misbehavior in MANETs was studied by Kejun Liu. The 2ACK scheme that serves as an add-on technique for routing schemes to detect routing misbehavior and to mitigate their adverse effect was presented. In order to send two-hop acknowledgement packets in the opposite direction of the routing path, the 2ACK scheme was used [5].

A proof-of-concept implementation of a secure routing protocol based on AODV over IPv6, further reinforced by a routing protocol-independent Intrusion Detection and Response system for ad-hoc networks was presented by Anand Patwardhan. The mechanisms for non-repudiation, authentication using Statistically Unique and Cryptographically Verifiable (SUCV) identifiers, without relying on the availability of a Certificate Authority (CA), or a Key Distribution Center (KDC) were included in the

security features of the routing protocol [6]. They have also discussed several scenarios where the secure routing and intrusion detection mechanisms isolate and deny network resources to nodes deemed malicious.

Li Zhao and José G. Delgado-Frias have proposed and evaluated a Multipath Routing Single path transmission (MARS) scheme to detect misbehavior on data and mitigate adverse effects. To provide more comprehensive protection against misbehavior from individual or cooperating misbehaving nodes, the proposed MARS scheme combined multipath routing, single path data transmission, and end-to-end feedback mechanism together [7].

Attacks against routing in ad hoc networks were presented by YihChun H. In addition, the design of Ariadne, a new secure on-demand ad hoc network routing protocol was presented and its performance was evaluated. Ariadne prevents attackers or compromised nodes from tampering with uncompromised routes consisting of uncompromised nodes. In addition, it prevents a large number of types of Denial-of-Service attacks [8].

Two techniques that improve throughput in an ad hoc network in the presence of nodes that agree to forward packets but fail to do so are presented by Sergio Marti. They have proposed categorizing nodes based upon their dynamically measured behavior to mitigate this problem. In order to identify the misbehaving nodes they employed a watchdog. In order to aid the routing protocols to avoid these nodes, a path rater was employed [9].

The SMT and SSP protocols for secure data communication in ad hoc networks were presented and analyzed by Panagiotis Papadimitratos and Zygmunt J. Haas. Owing to the fact that the two protocols provide lightweight end-to-end security services and operate without knowledge of the trustworthiness of individual network nodes, they are applied extensively [10].

An on-demand routing protocol for ad hoc wireless networks that provides resilience to byzantine failures caused by individual or colluding nodes was presented by Baruch Awerbuchl. After log n faults have occurred (where n is the length of the path), a malicious link is detected by their adaptive probing technique. Then, the weights of these links are multiplicatively increased and an on-demand route discovery protocol that finds a least weight path to the destination is utilized, hence these links are avoided [11].

The notion of a tunneling attack, in which collaborating malicious nodes can encapsulate messages between them to subvert routing metrics, was introduced by Kimaya Sanzgiri, et al. A solution for secured routing in the managed-open environment was provided by their protocol, ARAN. ARAN used pre-determined cryptographic certificates that guarantees end-to-end authentication to provide authentication and non-repudiation services [12].

The design and evaluation of SEAD, a secure ad hoc network routing protocol using distance vector routing was presented by Yih-Chun Hu, et. al. They used efficient one-way hash functions and did not use asymmetric cryptographic operations in the protocol to support use of nodes with limited CPU processing capability and to guard against Denial-of-Service (DoS) attacks in which an attacker attempts to cause other nodes to consume excess network bandwidth or processing time [13].

Gergely Acs [14] have argued that flaws in ad hoc routing protocols can be very subtle, and they advocated a more systematic way of analysis. They have proposed a mathematical framework in which security can be precisely defined and routing protocols for mobile ad hoc networks can be proved to be secure in a rigorous manner. Their framework was tailored for on-demand source routing protocols, but the general principles are applicable to other types of protocols too. Their approach was based on the simulation paradigm, which has already been used extensively for the analysis of key establishment protocols, but, to the best of our knowledge, it has not been applied in the context of ad hoc routing so far. They have also proposed an on-demand source routing protocol, called endairA, and demonstrated the use of our framework by proving that it is secure in our model.

Syed Rehan Afzal et al. [15] have explored the security problems and attacks in existing routing protocols and then they have presented the design and analysis of secure on-demand routing protocol, called RSRP. The proposed RSRP secure routing protocol was based on DSR, which uses a broadcast authentication scheme.

2.1 AODV Protocol Overview

The AODV [17, 18] routing protocol is a reactive routing Protocol; therefore, routes are determined only when needed. The message exchanges of the AODV protocol is given below.

Hello messages may be used to detect and monitor links to neighbors. If Hello messages are used, each active node Periodically broadcasts a Hello message that all its neighbors receive. Because nodes periodically send Hello messages, if a node fails to receive several Hello messages from a neighbor, a link break is detected.

When a source has data to transmit to an unknown destination, it broadcasts a Route Request (RREQ) for that destination. At each intermediate node, when a RREQ is

received a route to the source is created. If the receiving node has not received this RREQ before, is not the destination and does not have a current route to the destination, it rebroadcasts the RREQ. If the receiving node is the destination or has a current route to the destination, it generates a Route Reply (RREP). The RREP is unicast in a hop-by hop fashion to the source. As the RREP propagates, each intermediate node creates a route to the destination. When the source receives the RREP, it records the route to the destination and can begin sending data. If multiple RREPs are received by the source, the route with the shortest hop count is chosen.

As data flows from the source to the destination, each node along the route updates the timers associated with the routes to the source and destination, maintaining the routes in the routing table. If a route is not used for some period of time, a node cannot be sure whether the route is still valid; consequently, the node removes the route from its routing table.

If data is flowing and a link break is detected, a Route Error (RERR) is sent to the source of the data in a hop-by hop fashion. As the RERR propagates towards the source, each intermediate node invalidates routes to any unreachable destinations. When the source of the data receives the RERR, it invalidates the route and reinitiates route discovery if necessary.

3. On-Demand Byzantine-Resilient Secure Routing Protocol

In this section we describe our proposed protocol named On-Demand Byzantine resilient secure routing protocol.

3.1. Overview of the Protocol

We employ an authentication framework which eradicates a large class of outside attacks by ensuring that only authorized nodes can perform certain operations. Every node authorized to take part in the routing and data transmission is presented with a pair of public/private keys and a node certificate that connects public key of the node to its IP address. The token used to authenticate the nodes to be communicated in the network is periodically refreshed and disseminated by a special node, authorizer. Consequently, only the nodes that are currently participating in the routing or data forwarding operations will posses a valid tree token.

Both route request and route reply are flooded by the protocol which guarantees that a path is established even if route activation messages are dropped to mitigate inside attacks that try to prevent a node from establishing a route to the destination by employing a timeout based mechanism. If an adversarial-free route subsists, the protocol ensures the establishment of a route.

In order to provide resilience to selective data forwarding attacks, a reliability metric containing a list of link weights where high weights correspond to low reliability to capture adversarial behavior, is employed. Every node maintains its own weight list and includes it in each route request to ensure that a new route to the tree avoids adversarial links. The link's reliability is determined by the number of packets successfully delivered on that link. The destination node monitors the rate of receiving data packets and it is compared with the transmission rate specified by the source. If the variation amid the perceived transmission rate and the rate specified by the source on a link falls below a threshold value, the weight of that link is enhanced. Subsequently, the discovery of a new route is initiated.

3.2 Network Model and Authentication Framework

We consider a multi-hop wireless network where nodes participate in the data forwarding process for other nodes. We assume that the wireless channel is symmetric. All nodes have the same transmitting power and consequently the same transmission range. The receiving range of a node is identical to its transmission range. Also, nodes are not required to be tamper resistant: If an attacker compromises a node, it can extract all key material, data or code stored on that node.

We assume that nodes have a method to determine the source authenticity of the received data. The framework prevents unauthorized nodes to be part of the network or of the routing path. Each authorized node of the network has a pair of public/private keys and a node certificate that binds its public key to its IP address.

3.2.1 Secure Token Dissemination: The source node employs the pair-wise shared keys established between the neighbors to periodically refresh and broadcast the token used to authenticate all the nodes along the routing path. Hence, a valid token will be possessed by the nodes that are at present on the routing path. The source utilizes a one-way hash function F to periodically broadcast a token authenticator in the whole network. Nodes can apply the function F to the route token and compare it with the last received token authenticator to authenticate it.

3.2.2 Hop Count Authentication: Some malicious nodes will claim that they are at shorter hop distance from the source, though it is large. To prevent such nodes, a technique based on a hash chain similar to [6] is proposed. Let f be a one-way hash function and let dm be the maximum hop-distance of a path from a node to the source.

The source node S calculates the hop count index $HI = f^{dm}(X)$, where X is a random number selected by S. The source then includes the following information in the route request (RREQ) messages sent to the nodes:

$$[x, 0, dm, f^{dm}(X)]$$

Where the values dm and $f^{dm}(x)$ are digitally signed by the source.

A node along the routing path receives the following information from its parent:

$$[x, \mathrm{d}, \mathrm{dm}, \mathrm{f}^{\mathrm{dm}}(X)]$$

Where d is the parent's hop distance to the source and $f^{dm}(x)$ is the hop count index.

On receiving this information, the node verifies the signature on $(dm, f^{dm}(X))$ and checks if

$$f^{dm-d}(x) = f^{dm}(X).$$

If the above condition is satisfied, then the node forwards the packet with updated information, to its downstream nodes

$$[f(X), \mathrm{d}+1, \mathrm{dm}, \mathrm{f}^{\mathrm{dm}}(X)]$$

The one-way hash function f, prevents a node whose parent is d hops away from the source, to claim to be at a distance smaller than d+1 from the source.

The one-way hash function prevents a node whose parent is d hops away from the source, to claim to be at a distance smaller than d+1 from the source.

This hop count authentication mechanism is used by the source when sending route token. It is also used during route discovery to allow nodes that forward a route reply message to prove their hop distance from the node that initiated the route reply message.

3.3. Mitigating Inside Attacks during Route Discovery

A modified route request/route reply procedure utilized by the on-demand routing protocols is employed by the protocol. The route request (RREQ) message created by the source node and signed using its private key includes the node id, its weight list, and a request sequence number in a concatenated format. Subsequently, this signed RREQ message is broadcast to its one hop neighbors.

The destination node verifies whether the sequence number of RREQ received for the initial time from a node is lesser than its sequence number. If the sequence number of the destination node is greater, it validates the signature with its public key. If the signature is valid, it creates the RREP message that includes the node id, response sequence number, requester id and the weight list from the RREQ message. Besides, the node includes its current route token encrypted with the requester's public key to prove its identity. Furthermore, it includes the hop count authentication information to prove its hop distance to other nodes (see Sec. 3.2.2).

The RREP message is broadcasted towards the source by employing the following mechanism.

When a node receives this RREP message, it sums up the weight of all the links on the specified path from the destination to itself so as to compute the total path weight. Only if the total weight is less than any previously forwarded RREP message with same response sequence number, the hop count authentication and all the signatures collected on the response are considered to be valid. After the validation of the message, the node adds its id to the message and updates the hop count authentication information. Subsequently, the node signs the entire message and rebroadcasts it. While the RREP message propagates across the network, the nodes set pointers to the node from which the RREP was received in order to establish the forward route.

The procedure followed by the intermediate nodes during the RREP propagation when it receives a RREP is also performed by the source. Besides, the source verifies the validity of the route token included in the RREP message. The source updates its information, provided that it receives a valid RREP that contains a better path according to the reliability metric.

3.4. Selective Data Forwarding Attacks

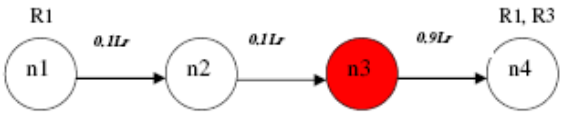

Fig.1 Selective Data Forwarding Attack

The source periodically broadcasts the data transmission rate R in a message (TR_MSG) after signing it. Nodes which receive this message, add their estimated transmission rate to the message and stores the copy of the last received TR_MSG. This message helps the node to detect the selective forwarding attack performed by the downstream nodes. It also adds its id, hop distance from the source and hop count authentication information (Sec. 3.2.2) along with its estimated rate.

Due to natural losses, the estimated rate of a node is smaller than the estimated rate of its parent node. As data transmission proceeds towards the destination, the rate is

further decreased. We define Lr as the threshold value for the tolerable loss rate, for a single link. Upon receiving a TR_MSG message, each node first checks if the difference between the last rate in TR_MSG and the node's estimated rate is greater than a threshold value β, where β=2*R . If so, this indicates that there exists at least a malicious node in between this node and the node that added the last rate to TR_MSG . The first trustworthy node that notices a difference larger than β, penalize the link to its parent as defective or malicious and assumes responsibility for finding a new route to the destination. Notice that in fig. 1, if node n3 is malicious, it adds the rate as 0.9R. Then at n4, it checks, if $R4 - R1 > \beta$. if it is greater , it penalize the link $n3 - n4$ .The entire TR_MSG is signed by the node and forwarded to the next hop node. When a node receives this message, it checks the validity of the hop count authentication information and verifies the aggregated signatures. After verification, it forwards the message to the downstream node.

4. Performance Evaluation

4.1Simulation Model and Parameters

We use NS2 to simulate our proposed algorithm. In our simulation, the channel capacity of mobile hosts is set to the same value: 2 Mbps. We use the distributed coordination function (DCF) of IEEE 802.11 for wireless LANs as the MAC layer protocol. It has the functionality to notify the network layer about link breakage.

In our simulation, 50 mobile nodes move in a 1000 meter x 1000 meter rectangular region for 50 seconds simulation time. We assume each node moves independently with the same average speed. All nodes have the same transmission range of 250 meters. In our simulation, the minimal speed is 5 m/s and maximal speed is 10 m/s. The simulated traffic is Constant Bit Rate (CBR). We vary the no. of misbehaving nodes as 5, 10, 15 and 20.

Our simulation settings and parameters are summarized in table 1

No. of Nodes	50
Area Size	1000 X 1000
Mac	802.11
Radio Range	250m
Simulation Time	50 sec
Traffic Source	CBR
Packet Size	512 KB/s
Speed	5m/s t 10m/s
Misbehaving Nodes	5,10,15 and 20

4.2 Performance Metrics

We evaluate mainly the performance according to the following metrics.

Control overhead: The control overhead is defined as the ratio between total numbers of routing control packets to the total number of received data packets.

Average end-to-end delay: .The end-to-end-delay is the average time taken by data packets to reach from the sources to the destinations. This includes all the delays caused during route acquisition, buffering and processing at intermediate nodes, retransmission delays at the MAC layer, etc.

Average Packet Delivery Ratio: This is the fraction of the data packets generated by the sources that are delivered to the destination. This evaluates the ability of the protocol to discover routes [12]

Node Reliability: The node reliability is calculated by the packet delivery ratio of that particular node. If the ratio is high means reliability is also high.

Resistance against Node Capture: Here we are going to calculate how a node capture attack affects the performance of the protocol.. It is calculated by estimating the fraction of communications compromised between non compromised nodes by a capture of x-nodes.[16]

Let $P_e(C)$ is the probability that an adversary can access the secret communication between two non-compromised nodes U and V when C nodes are already being captured.

If $P_e(C) = 0$, then we call the routing protocol is unconditionally secure and having high resistance against node capture

The simulation results are presented in the next section. We compare our BRSR with the AODV-SEC [6] protocol in presence of malicious node environment.

4.3 Results

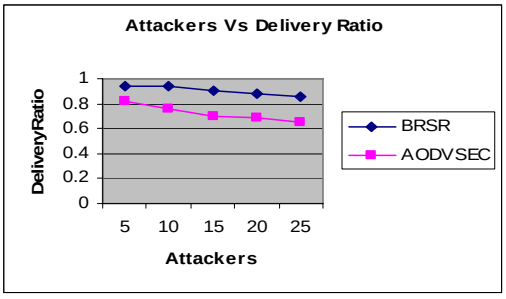

Fig. 2 Attackers Vs Delivery Ratio for 50 nodes

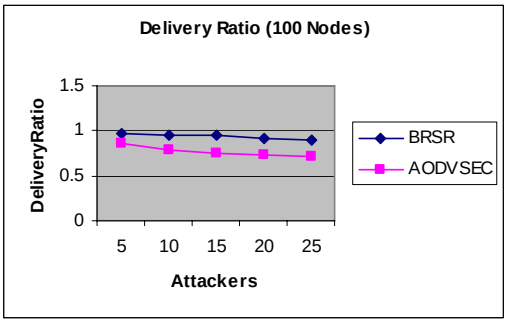

Fig. 3 Attackers Vs Delivery Ratio for 100 nodes

Figures 2 and 3 show the results of average packet delivery ratio for the misbehaving nodes 5, 10,….25 for 50 nodes and 100 nodes scenario respectively. Clearly our BRSR scheme achieves more delivery ratio than the AODV-SEC scheme since it has more security features.

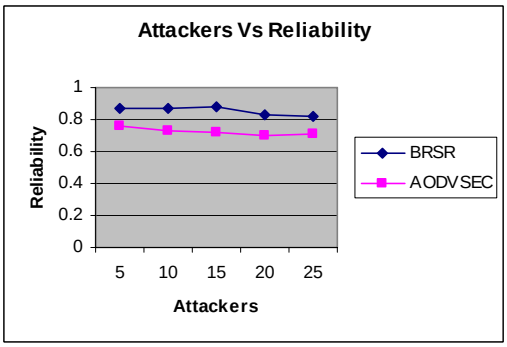

Fig. 4 Attackers Vs Reliability

Fig. 4 shows the results of reliability for the misbehaving nodes 5,10,….25 for 50 nodes scenario. Clearly our BRSR scheme achieves more reliability than the AODV-SEC scheme since it has better delivery ratio compared with AODV-SEC.

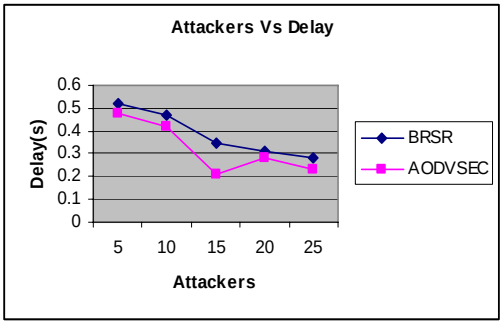

Fig. 5 Attackers Vs Delay

Fig. 5 shows the results of average end-to-end delay for the misbehaving nodes 5, 10,….25. From the results, we can see that BRSR scheme has slightly higher delay than the AODVSEC scheme because of authentication routines and the security features that the protocol is having.

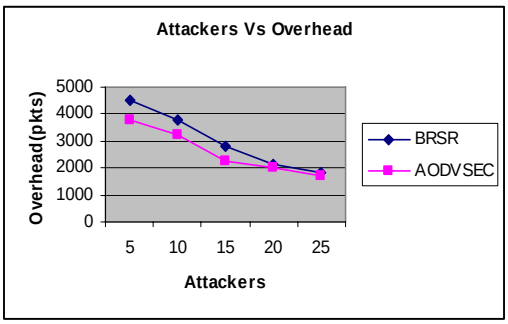

Fig. 6 Attackers Vs Overhead

Fig. 6 shows the results of routing overhead for the misbehaving nodes 5,10,….25. From the results, we can see that BRSR scheme has more routing overhead than the AODVSEC scheme since involves route re-discovery routines..

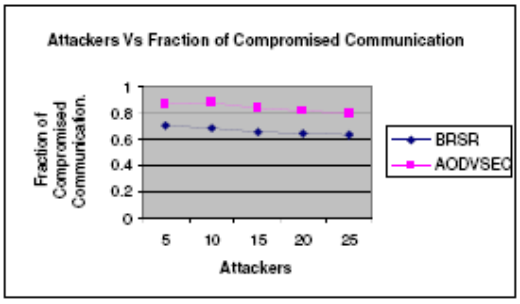

Fig. 7 Attackers Vs Fraction of Compromised Communication

Fig. 7 shows the fraction of compromised communications for the non-compromised nodes. With increase in the number of attackers from 5 to 25 attackers, the ratio is less for BRSR when compared to AODV-SEC. This means the probability that an adversary can access the secret communication between two non-compromised nodes is less for BRSR compared with AODV-SEC. That is BRSR protocol is more secure and having high resistance against node capture than AODV-SEC.

5. Conclusion

In mobile adhoc networks, the Byzantine behavior of authenticated nodes results in route disruption actions. To mitigate these vulnerabilities of routing protocols in

wireless adhoc networks, we propose a new Byzantine-Resilient Secure Routing Protocol (BRSR) that provides resilience against Byzantine attacks. Since existing routing protocols provide solutions separately for insider attacks, outsider attacks and selective forwarding attacks, our proposed protocol provides total protection against all these attacks. Through simulation results, we have demonstrated that BRSR effectively mitigates the identified attacks with stronger resistance against node capture by providing better delivery ratio. As a future work, we will try to reduce the overhead and delay of the proposed protocol by maintaining much more resistance against the identified attacks.

References

[1] H Yang, H Y. Luo, F Ye, S W. Lu, L Zhang, "Security in mobile ad hoc networks: Challenges and solutions", IEEE proceedings on wireless Communications, vol.11, no.1, pp: 38-47, Feb. 2004, Doi: 10.1109/MWC.2004.1269716.

[2] Ovais Ahmad Khan, "A Survey of Secure Routing Techniques for MANET", Course Survey Report, Fall 2003.

[3] Tarag Fahad & Robert Askwith, "A Node Misbehaviour Detection Mechanism for Mobile Ad-hoc Networks",

[4] Yanchao Zhang, Wenjing Louy, Wei Liu and Yuguang Fang, "A Secure Incentive Protocol for Mobile Ad Hoc Networks", in proc. of Journal on Wireless Networks, vol. 13, no. 5, pp: 569- 582, October 2007.

[5] Kejun Liu, Jing Deng, Pramod K. Varshney, and Kashyap Balakrishnan, "An Acknowledgment-based Approach for the Detection of Routing Misbehavior in MANETs", IEEE Transactions on Mobile Computing, vol. 6, no. 5, pp: 536-550, May 2007.

[6] Anand Patwardhan, Jim Parker and Anupam Joshi, "Secure Routing and Intrusion Detection in Ad Hoc Networks", in proc. of 3rd International Conference on Prevasive Computing and Communications, March 8, 2005.

[7] Li Zhao and José G. Delgado-Frias, "MARS: Misbehavior Detection in Ad Hoc Networks", in proc. of IEEE Conference on Global Telecommunications, pp: 941-945, 26- 30 Nov. 2007, Doi: 10.1109/GLOCOM.2007.181.

[8] YihChun Hu, Adrian Perrig and David B. Johnson, "Ariadne: A Secure On-Demand Routing Protocol for Ad Hoc Networks", in Wireless Networks (WINET), ACM and Springer, 11(1-2):21-38, January 2005.

[9] Sergio Marti, T.J. Giuli, Kevin Lai, and Mary Baker, "Mitigating Routing Misbehavior in Mobile Ad Hoc Networks", in proc. of 6th Annual International Conference on Mobile Computing and Networking, pp: 255- 265, 2000.

[10] Panagiotis Papadimitratos and Zygmunt J. Haas, "Secure Data Communication in Mobile Ad Hoc Networks", in proceedings of IEEE Journal on Selected Areas in Communications, vol. 24, no. 2, February 2006.

[11] Baruch Awerbuch, David Holmer, Cristina NitaRotaru and Herbert Rubens, "An On Demand Secure Routing Protocol Resilient to Byzantine Failures", in proc. of 1st ACM workshop on wireless security, pp: 21- 30, 2002.

[12] Kimaya Sanzgiri, Bridget Dahill, Brian Neil Levine, Clay Shields and Elizabeth M. Belding-Royer, "A Secure Routing Protocol for Ad Hoc Networks", in proc. of 10th International Conference on Network Protocols, pp: 78-87, 12-15 November 2002.

[13] Yih-Chun Hu, David B. Johnson and Adrian Perrig, "SEAD: Secure Efficient Distance Vector Routing for Mobile Wireless Ad Hoc Networks", in proc. of 4th IEEE Workshop on Mobile Computing Systems and Applications, pp: 3-13, 2002, Doi: 10.1109/MCSA.2002.1017480.

[14] Gergely Acs, Levente Buttyan, and Istvan Vajda, "Provably Secure On-Demand Source Routing in Mobile Ad Hoc Networks", IEEE Transactions on Mobile Computing, vol. 5, no. 11, November 2006.

[15] Syed Rehan Afzal, Subir Biswas, Jong-bin Koh, Taqi Raza, Gunhee Lee, and Dong-kyoo Kim, "RSRP: A Robust Secure Routing Protocol for Mobile Ad hoc Networks", in proc. of IEEE Conference on Wireless Communication and Networking, pp: 2313- 2318, March 31- April 3,Las Vegas, NV, 2008, Doi: 10.1109/WCNC.2008.408.

[16] Adrian Perrig, John Stankovic, and David Wagner "Security in Wireless Sensor Networks". In the proceedings of Communications of the ACM June 2004/vol/47 No.6page no 53-57.

[17] C. E. Perkins, E. M. Belding-Royer, and S. Das. Ad hoc On- Demand Distance Vector (AODV) Routing. *RFC 3561*, July 2003.

[18] C. E. Perkins and E. M. Royer. The Ad hoc On-Demand Distance Vector Protocol. In C. E. Perkins, editor, *Ad hoc Networking*, pages 173.219. Addison-Wesley, 2000.

Saju P John received the B-Tech Degree in Computer Science from Calicut University, the M.E Degree in Computer science from Anna University and presently doing part time Ph D in Cochin University of Science & Technology India. He is presently working as Assistant professor in Computer Science & Engineering Department, Thejus Engineering College, Thrissur India 680584. His Current research interests include Network security, Mobile Communication, Adhoc networks etc.

Philip Samuel received the M.Tech degree in Computer Science from Cochin University and the PhD degree from IIT Khargpur. He is presently working as Head of Information Technology division, School of Engineering, Cochin University of science & Technology, India 682002. His Current research interests include, University of science & Technology, India 682002. His Current research interests include, Networking, Object oriented modeling &Design, Software Engineering Mobile Communication, Adhoc networks etc.