PERFORMANCE ANALYSIS OF SECURED POSITION BASED ROUTING IN MOBILE AD HOC NETWORKS

1B. Rammyaa 2Dr.K.S.Vishvaksenan 3Dr.SumathiPoobal

Address for Correspondence
1Asst.Professor-Department of EIE, KCG College of Technology
2Associate Professor-Department of ECE,SSN College of engineering
3Professor and Head-Department of ECE,KCG College of Technology

ABSTRACT
Mobile Ad hoc Networks are used particularly in critical applications that lack fixed Network infrastructure. The geographical information used by routing protocols makes forwarding decision for reduced routing. But the topology based MANET protocols are vulnerable to number of attacks. As position based routing protocols concentrate on improving the performance, they fail to concentrate on the security issues. Current position based routing allows anyone within the range to receive the position information and cannot be designed for use in high risk environment. If lots of authentication techniques are implemented, the battery power of the nodes gets exhausted. Because of some special characteristics of MANETs, prevention mechanism alone is not satisfied to manage the secure network. Detection of attack and security should be focused before an attacker can damage the structure of the system. The objective of the paper is to compare the performance of different secured position based routing protocols to find solution for secured routing.

KEYWORDS: MANETs, Routing Protocols, Position Based Routing, Security issues, Authentication techniques, Secured Routing.

1. INTRODUCTION
A mobile Ad hoc network (MANET) is a collection of wireless mobile nodes self-configured to form an infrastructure less network. It is important that the routing protocol should be able to find routes that have a high degree of mobility. The challenges to the routing protocol design are the lack of dedicated routing infrastructure. Routing is the process of finding a path from a source to some arbitrary destination on the network. Existing routing protocols can be classified either as proactive or reactive. Routing in MANET is an important issue as it involves sending messages to a destination node in a network. As each node move arbitrarily in MANET, it causes the network topology unpredictable as it change frequently. These characteristics make the designing of routing protocol more complicated for MANET. MANETs can quickly set up as needed and they need secure routing than any other network due to lack of infrastructure and broadcast nature of the network. Position based routing protocols can offer significant location discovery will be able to identify and discard replies providing false topological information or avoid receiving them. Any two nodes that wish to communicate securely can establish a shared secret key for encryption and decryption. That makes position discovery to be protected. Secure routing protocols protects routing messages against malicious nodes.

2. REVIEW OF SECURED POSITION BASED ROUTING PROTOCOLS
Position changes which occur because of nodes mobility in MANET cause changes in routing tables of nodes. Localization is realized by GPS that is used to determine geographical positions of nodes. The GPSs, which are embedded in nodes, are used to update information in tables in position-based algorithms. That makes position-based algorithms different from the table driven and on demand algorithms. Routing protocols uses geographical information to make forwarding decisions, resulting in reduced routing.

One of the primary applications of MANETs is in military use. In high risk environment, position information broadcasted allows anyone including enemy within the range to receive the information. So the position used in MANET routing protocols are to be protected. Secure routing protocols protects routing messages against malicious nodes.

2.1 Secure Routing Protocol (SRP)
In [9], Papadimitratos and Haas propose the Secure Routing Protocol (SRP) as a solution for securing MANET. SRP requires a security association between the source and destination nodes and asserts that SRP guarantees the node initiating a route discovery will be able to identify and discard replies providing false topological information or avoid receiving them. Any two nodes that wish to communicate securely can establish a shared secret key for encryption and decryption. That makes position discovery to be protected. Secure routing protocols protects routing messages against malicious nodes.

Figure 1. Example for SRP routing
The source node will not choose the shortest path because it believes in the false path of 3 hops. If this false path is chosen, the malicious nodes negatively impact the network performance by delaying or dropping packets. The protocol violates security...
deployed by a known source. A compromised node unauthorized node disrupts the network. SPAAR uses compromised nodes. It is important to distinguish malicious nodes from nodes, and malicious nodes are a constant threat. It is for the pre-deployment coordination. SPAAR targets an environment similar to deployment coordination. SPAAR was designed for use in a specific environment. In [2], the ad hoc networks are classified into three environments: open, managed-open, and managed-hostile. Each environment differs in its security needs and opportunity for pre-deployment coordination. SPAAR targets an environment similar to managed-hostile environment. The managed-hostile environment is described as a MANET formed by military nodes in a battle environment or similarly an emergency response crews in a disaster area. Nodes are generally deployed from a common source and the opportunity for the pre-deployed security parameter exchange often exists. Sensitive information is passed between nodes, and malicious nodes are a constant threat. It is important to distinguish malicious nodes from compromised nodes. A malicious node to be an unauthorized node disrupts the network. SPAAR uses encryption to prevent attacks, though at the expense of performance and resource consumption. A compromised node to be an authorized node deployed by a known source. A compromised node may or may not engage in malicious activity or misbehave. As a result, detection of compromised nodes can be very difficult. In many cases it is difficult to distinguish malicious activity by a compromised node from legitimate node activity. SPAAR protects a MANET from attacks by malicious nodes, while attempting to minimize the potential for damage by attacks originating from compromised nodes. While SPAAR does not defend against all malicious activity from compromised nodes, ad hoc intrusion detection systems [9] can help to identify compromised nodes. SPAAR provides the necessary elements to secure routing in a high-risk environment: authentication, non-repudiation, confidentiality, and integrity. The protocol protects position information via cryptographic techniques. The protected position information is used to reduce routing overhead and increase the security of routing.

2.4 Security Grid Location Service Forwarding (SGLSF)

The SGLSF [16] mechanism combines Secure Geographic Forwarding (SGF) [17] and Grid Location Service (GLS) [8]. The SGF mechanism uses the shared key and the Timed Efficient Stream Loss-tolerant Authentication (TIK) [18] protocol to provide source authentication, neighbor authentication, and message integrity by incorporating hashed message authentication code (MAC). By combining these SGF and GLS, SGLSF, enhances the security to the original protocol to ensure that any receiver can authenticate the accuracy of location messages. GLS has the ability to message tampering, dropping, falsified injection, and replay attacks. The Local Reputation System (LRS) find compromised and selfish users and isolate messages by dropping attackers from the network. Both mechanisms combined; continue to maintain a larger message delivery ratio at the expense of a slightly higher average end-to-end delay and routing overhead compared to when they are not combined. SGLS can operate efficiently by using effective cryptographic mechanisms.

2.5 Secure Adhoc Routing Protocol

<table>
<thead>
<tr>
<th>Name of Approach</th>
<th>Protocol</th>
<th>Assumption</th>
<th>Result Optimisation</th>
<th>Technique Used</th>
</tr>
</thead>
<tbody>
<tr>
<td>Secure position based routing protocol(Hybrid)</td>
<td>SGF</td>
<td>Effective cryptographic mechanism</td>
<td>Source authentication, Neighbor authentication and message integrity</td>
<td>Ns-2 simulator</td>
</tr>
<tr>
<td>Secure Position Aided Adhoc Routing (SPAAR)</td>
<td>SPAAR</td>
<td>Cryptographic techniques</td>
<td>Authentication, privacy , overall routing overhead reduction and integrity</td>
<td>Asymmetric Cryptography</td>
</tr>
<tr>
<td>Five Layer Security Architecture</td>
<td>Pseudo AODV protocol</td>
<td>Security architecture for MANETs</td>
<td>Designing security architecture, tackling security challenges</td>
<td>Case study of five layered architecture</td>
</tr>
<tr>
<td>Privacy-Preserving Location-Based On-Demand Routing</td>
<td>PRISM</td>
<td>Location centric Communication</td>
<td>Privacy, security, efficiency and Authenticate node</td>
<td>Network simulator</td>
</tr>
<tr>
<td>Secure Routing Protocol for securing MANETs</td>
<td>SRP</td>
<td>Data and trusted values routed through trusted routes</td>
<td>Discards false topological information</td>
<td>Secure Routing in RREQ</td>
</tr>
<tr>
<td>Security aware Ad hoc routing for Wireless Network</td>
<td>SAR</td>
<td>Nodes with security level participate in routing</td>
<td>Flexible and Prevent Attacks</td>
<td>Network Simulator</td>
</tr>
<tr>
<td>Secure On-Demand Position-Based Ad Hoc Routing</td>
<td>AODV protocol</td>
<td>Adaptive Routing, Autonomous Position verification system, Trust factor evaluation ,secure neighbor detection</td>
<td>Enhance security level of discovered path, overcome warm hole attack</td>
<td>DES encryption mechanism to secure the field in routing packets</td>
</tr>
</tbody>
</table>
Most of the attacks on routing protocol are due to absence of Encryption. Unauthorized modification of such fields could cause serious security threats. DES for encryption mechanism is used. Each node in the network maintains a public/private key pair; the certificate is to be valid for certain time period. Each node has T’s public key, so it can decrypt certificates of other nodes. The protocol overcomes all known vulnerabilities of the existing protocols. It uses DES encryption mechanism to secure the fields in routing packets. The most severe attacks on MANETs is warmhole attack.

This can be overcome applying efficient secure neighbor detection mechanism. To enhance the security level of discovered path, route selection is done based on trust level of nodes along the path. In order to secure position coordinates of each node Position verification system is employed. Based on the basic operation of AODV as in figure 2, the security level is required by application. In mode 1, the packets are routed along the trusted path based on the trust factor of the nodes. In mode 2, the packets are routed along the shortest path based on hop count. The protocol uses a mechanism to detect and overcome the effect of falsified position information in geographic routing position. The protected position information reduces the routing overhead and increase the security of routing

![Adaptive Routing](image)

The designing of security architecture [6] for tackling security challenges in mobile ad hoc networks are discussed. The security architecture in a layered view is analyzed for applying the security architecture in military scenarios. It can be used as a framework when designing system security for ad hoc networks. An efficient secure routing protocol for mobile ad hoc networks guarantees the discovery of correct connectivity information over an unknown network, in the presence of malicious nodes. The term of anonymous location-based routing occur in certain types of suspicious MANETS. It relies on group signatures to construct one-time pseudonyms used to identify nodes at certain locations.

The framework works with any group signature scheme and any location-based forwarding protocol can be used to route data between nodes. Also alternate routes are utilized only when data packets cannot be delivered through the primary route. As a case study, this algorithm is applied to AODV for performance enhancement.

3. COMPARISON OF PROTOCOLS

Secure communication is a major concern in wireless ad hoc networks due to the broadcast nature of the network, the existence of a wireless medium and the lack of any Centralized infrastructure. Multicast routing protocols should take this into account, especially because some of these protocols are applied in areas such as military (battlefield) operations, national crises, and emergency operations. The unique characteristics of MANETs, combined with security threats, demand solutions for securing ad hoc networks prior to their use in commercial and military applications. Some of the unique characteristics of MANETs that pose a strong challenge to the design of the secure multicast routing protocols include: open peer-to-peer network architecture, shared wireless medium, demanding resource constraints, and dynamic network topology.

Routing is a challenging aspect of moving packets around in a network. It is a significant problem because any node can perform the role of the router in MANET and security concepts were not included into the routing protocols when they were designed. It is important because the routing table forms the basis of the network operations. The comparison of various algorithms based on their routing protocols, mechanism and optimization of the result is done in Table 1. Each algorithm has its own pros and cons. Among several security protocols, no approach fit for all networks, because the nodes can vary between any devices.

<table>
<thead>
<tr>
<th>PROTOCOLS</th>
<th>Routing approach</th>
<th>Routing Protocol</th>
<th>Security Mechanism</th>
</tr>
</thead>
<tbody>
<tr>
<td>ARIADNE</td>
<td>Reactive</td>
<td>Based on DSR</td>
<td>Symmetric key cryptography</td>
</tr>
<tr>
<td>ARAN</td>
<td>Reactive</td>
<td>Based on AODV,DSR</td>
<td>Asymmetric Key Cryptography</td>
</tr>
<tr>
<td>SEAD</td>
<td>Proactive</td>
<td>Based on DSDV</td>
<td>One way Hash function</td>
</tr>
<tr>
<td>SAODV</td>
<td>Reactive</td>
<td>Based on AODV</td>
<td>Asymmetric key cryptography, one way hash function</td>
</tr>
<tr>
<td>SRP</td>
<td>Reactive</td>
<td>Extension Compatible with DSR</td>
<td>Security association between source and destination</td>
</tr>
</tbody>
</table>

MANETs lack fixed infrastructure and nodes are powered by batteries with a limited energy supply. Nodes stops functioning when the battery drain, it is a difficult challenge to provide energy efficiency as it is impossible to recharge or replace a mobile node, powered by battery during mission. Hence energy
efficiency is an important consideration. Traffic should be routed in the way energy consumption is minimized. Energy saving techniques aim at minimizing total power consumption. This can be done by minimizing the control overhead, maximizing the lifespan.

4. PROPOSED SECURE POSITION BASED ROUTING ALGORITHM

Due to high mobility of nodes, the network topology of MANET changes very fast. It is important to reduce disruption caused by changing topology. Link expiration does not provide security. So connectivity of mobile nodes till message reaches the destination and protection against various security attacks need to be proposed. As nodes can join & leave the network anytime, it leads to frequent change in topology of the network & making MANETs vulnerable to security attacks. The comparison of Protocols and their attacks are given in Table 2 and Table 3 respectively.

**TABLE 2: COMPARISON OF PROTOCOL WITH ATTACK**

<table>
<thead>
<tr>
<th>Protocols</th>
<th>Wormhole</th>
<th>Spoofing attack</th>
<th>Black hole Attack</th>
<th>DOS attack</th>
<th>Rushing attack</th>
</tr>
</thead>
<tbody>
<tr>
<td>ARIADNE</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>ARAN</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>SEAD</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>SAODV</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>SRP</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>

An additional advantage of the proposed algorithm is that any node except master node does not hold routing table and the process of routing determination since only master nodes responds to routing requests. As a result of this, life times of batteries of nodes will be longer. The performance of Secured PBHRA algorithm when compared to AODV, DSR, DSDV is given in figure 3.

The simulation study for evaluating the proposed algorithm can be extended by considering security issues. The performance comparison of secured PBHRA algorithm with different nodes is given in figure 4 and Screenshot of PBHRA with 50 nodes is given in figure 5. The Simulation study is done in 300 seconds using Qualnet Simulation tool.

6. CONCLUSION

An overview of existing scenario of the routing protocols for MANETs, based on their position based secured routing is presented. Each protocol has its own advantages and limitations. The problems that exist in the network and their emerging solutions are discussed. Also a comparative study of the protocols based on Secure Position Based Routing for maintaining the location privacy routing along with efficiency of the algorithm is done. It is difficult task to compare the protocols with each other directly. Since each protocol differ in their assumption and mechanism for achieving their goal. Each protocol has its own strength and drawbacks. Ad hoc networks gain many applications today; also it’s a wide area of research with the problems and emerging solution.
REFERENCES


