Volume-02
Issue-01
Feb-2019

ISSN: 2663-0931(Print)
ISSN: 2663-2594(online)
International Journal of
Interdisciplinary Current Advanced Research
www.ijicar.in

Securing communication channel with SUCV in Ad-hoc networks

*1Mr..Rajesh A,

*1 Student, International institute of Information technology, Hinjewadi, Pune, India.
Note: * Indicates corresponding author

ARTICLE DETAILS

Article History:
Received Date:11/02/2019
Revised Date: 16/02/2019
Accepted Date:25/02/2019
*Published Online:*10/03/2019

Keywords
Mobility, Trust information,
Manets, KDC, C.A,SUCV, SecAODV

*Corresponding Author
(A.Rajesh)

ABSTRACT

Ad hoc networks are a special kind of wireless network mode. Mobile ad hoc networks (MANETs) are self-organizing networks that do not require a fixed infrastructure. All nodes of MANETs are mobile hosts with similar transmission power and computation capabilities. The feature having no fixed infrastructure makes MANETs to exhibit two antagonistic characteristics. For instance, this feature popularize MANETs to be deployed at some place where wired networks are impossible to be laid down on one hand, this feature also renders MANETs in jeopardies that attackers can easily break-in on other hand. In this paper, we present a proof-of-concept implementation of a secure routing by using SUCV for ad-hoc networks. Although many deployments of MANETs are highly sensitive to the message transmitted in the application layer, MANETs often lack security mechanism in place within the network layer or MAC layer. For instance, MANETs are vulnerable to many kinds of attacks with IEEE 802.11 standard in MAC and PHY layers. The mobility of hosts within MANETs adds another dimension of complexity in the network layer such as routing and security. Security features in the routing protocol include 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).

1. Introduction

Wireless networks generally are more vulnerable to link attacks than wired networks due to the wireless transmission media. A scrutiny's reveals that security concerns in wireless networks involve two separate problems: secure routing discovery and secure data transmission over the wireless networks. MOBILE ad hoc networks (MANETs) aim to provide wireless network services without relying on any infrastructure. The main challenge in MANETs comes from their self-organized and distributed nature[5]. There is an inherent reliance on collaboration between the participants of a MANET in order to achieve the aimed functionalities.

Collaboration is productive only if all participants operate in an honest manner. Therefore, establishing and quantifying trust, which is the driving force for collaboration, is important for securing MANETs. Trust can be defined as the firm belief in the competence of an entity to act dependably, securely, and reliably within specified context[**8**]. It represents a MANET participant's anticipation of other nodes' behavior when assessing the risk involved in future interactions. Here, the participant is usually called the trustor, and other nodes are called the trustee. The trust relationship usually builds on the basis of the trustor's past direct interaction experiences and others' recommendations related to the trustee. The abstracted value from past experiences and recommendations is defined as the trustee's reputation. Ad hoc networks are comprised of a dynamic set of cooperating peers, which share their wireless capabilities with other similar devices to enable communication with devices not in direct radio- range of each other, effectively relaying messages on behalf of others. Conventional methods of identification and authentication are not available, since the availability of a Certificate Authority or a Key Distribution Center cannot be assumed.

Consequently, mobile device identities or their intentions cannot be predetermined or verified. Several routing protocols for ad-hoc networks have been proposed like DSDV, DSR, AODV, TORA etc[2,3,7]. A majority of these protocols assume a trustworthy collaboration among participating devices that are expected to abide by a "code-of-conduct"[5].

2. Previous Works In existing System inherent vulnerabilities of mobile devices in MANETs and several attacks possible on such devices. They developed a practical solution to the secure routing on MANETs.

Even after protecting the network from

routing disruption attacks, packet mangling attacks and grey holes, denial of service attacks that use MAC vulnerabilities to disrupt communication are still possible.

3. Our approach At First we have to see the Nodes can operate on their own, Secondly, based on the characteristics of MANETs and the requirements of secure routing, FL-SAODV, a new secure and efficient routing protocol has been developed. A set of algorithms have been designed for FL-SAODV. Thirdly, these algorithms have been implemented on the MANETs and many experiments on different scenarios have been carried out on NS2. Lastly, we listed out the security level of the nodes which are on the final route. The route found by using the FL-SAODV protocol have higher security level than the route AODV found.

Algorithm FL-SAODV Route Discovery

```
S ← SourceNode, D ← DestinationNode
$SL_i$ is the security level of node i.
$SL_p$ is the security level in the RREQ packet
{ The Destination node sends RREP back}
Source node broadcasts a RREQ to all of its neighbors
repeat
  for neighbor nodes do
    if there is a route to the destination node then   authenticate the RREQ using MD5
      If  $SL_i > SL_p$ then
        update the security level in the RREQ packet
        overwrite the SL in RREQ packet with
        $S_{ij} = \min( S_{ij}, SL_p )$
        update other fields in RREQ
      end if
    else
      broadcast the RREQ to its neighbor nodes
    end if
  end for
```

In this algorithm, movement is calculated based on distance. If **SL_i** is within threshold then it is called micro mobility. Micro mobility doesn't require confirmation from supervisor. Because movement is within distance. But Macro mobility requires confirmation from nearest supervisor. This supervisor acts as Foreign agent from one place to another place. All nodes will store mobile behavior but supervisor will store particular opinion only.

Algorithm 2. Create and Unicast

```
for all RREQ received do
  if Broadcast ID && Security Level in RREQ then
    create a RREP packet
    unicast RREP back to S
  else
    drop the RREQ
  end if
  the destination determines which route is the best
  $SL_K = \max ( S_i )$
end for
```

This algorithm shows counter increment. If counter meets threshold then node broadcasts information to all nodes including supervisor. And it starts moving. The moving nodes repeat the local contact process after they arrive in the capital. The pause time period in the capital allows them to build trust between each other and the local nodes of the capital. One node, which is commonly trusted by all moving nodes, will be elected to be the keeper of that region through a process similar to Algorithms 1 and 2. The keeper selects several nodes it trusts as supervisors, which will travel between regions to collect information and feed it back to the keeper.

4. Working of SAODV over IPv6

We describe an implementation of FL-SAODV, built as an augmentation to the SAODV protocol in the NS2 network simulator. The AODV protocol, as proposed by RFC 3561, is comprised of two basic mechanisms, viz. route discovery and maintenance of local connectivity mechanisms. The Route Discovery mechanism is employed in an “Ad Hoc,

On Demand” fashion. The source node S - the device that requests communication with another member of the MANET referred to as destination D - initiates the process by constructing and broadcasting a signed route

request message RREQ. The format of the RREQ message differs from the one proposed. An AODV message contains the RSA public key of the source node S and that it is digitally signed to ensure the node’s authentication and message integrity.

4.1 Routing table

Every entry in the routing table contains seven fields as follows, **[6, 10]**

1 Destination IP Address

2 Destination Sequence Number

3 Valid Destination Sequence Number flag

4 Security Level

5 Hop Count

The field of Security Level is an additional than the ones in the routing table of AODV protocol. It is designed to represent the minimum security level of all nodes in the route. The field of list of precursors contains those neighboring nodes to which a route reply was generated or forwarded. In our implementation, a data structure called linked list which represents the expiration time of the route,**[1]** the field of Hop Count is the number of hops needed to reach the destination. **RREQ** message, each node member of the MANET authenticates the source node S and verifies message integrity by checking the IP address using the same secure bootstrapping algorithm.**[9]** The route

Maintenance of Local Connectivity mechanism is optionally achieved by periodically broadcasting Hello-type messages. In our implementation these messages are signed and contain the sender’s public key for authentication and message integrity verification. Additional information on local connectivity maintenance can be found. During our implementation and testing of AODV and Sec AODV, we observed that the protocol’s

performance is very sensitive especially to the **HELLO INTERVAL** and all parameters related to it: **ACTIVE ROUTE TIMEOUT, DELETE PERIOD, MY ROUTE TIMEOUT** are described.**[2,3,8].**

Protecting routing information from attackers by using hop-by-hop authentication technique : digital signature and hash. This avoids using a CA where other secure routing protocols have to.

1. It can adapt itself to the changing environment which is the most salient characteristics of the MANETs.

2. FL-SAODV also improves MANETs security from two aspects:

- It selects the shortest route which decreases the transmitting time and therefore could shorten the attack time of attackers and improve the MANET’s security.

- Using security level as metric ensures the updated route to be the most secure one.

5. Conclusion

First of all, the inherent vulnerabilities of mobile devices in MANETs and several

attacks possible on such devices. we have reviewed the possibility of attacks to the MANETs, and the security adversaries which compromise a mobile host in ad hoc networks for the purpose of identifying a strategy to beef up hosts security level. Secondly, based on the characteristics of MANETs and the requirements of secure routing, FL-SAODV, a new secure and efficient routing protocol has been developed. A set of algorithms have been designed for FL-SAODV. Thirdly, these algorithms have been implemented on the MANETs and many experiments on different scenarios have been carried out on NS2. Lastly, we listed out the security level of the nodes which are on the final route. The route found by using the FL-SAODV protocol has higher security level than the route AODV found. In addition, we shown the timings on its en route nodes and clearly shown that each route node needs more time than AODV to decide their next hop. There are two open questions for our future research. We believe that the performance of the protocol might be improved by using a better authentication method on one hand. On another hand, how to get the knowledge about the number of neighbor nodes needs more study.

References

1. Anand Patwardhan, Jim Parker, Anupam Joshi, Michaela Iorga and Tom Karygiannis, “Secure Routing and Intrusion Detection in Ad Hoc Networks”
2. D.B. Johnson, D. M. & Hu, Y. (2003). The dynamic source routing protocols for mobile ad hoc networks (DSR).
3. C. Perkins and E. Belding-Royer and S. Das. “Ad hoc On-Demand Distance Vector (AODV) Routing”, July 2003.
4. Hu, Y. C., Perrig, A. & Johnson, D. B. (2002). Ariadne: A secure on-demand routing protocol for ad hoc networks.
5. J. Wu, F. Dai, M. Gao, and I. Stojmenovic, “On Calculating Power-Aware Connected Dominating Sets for Efficient Routing in Ad Hoc Wireless Networks,” J. Comm. and Networks, vol. 4,no. 1, pp. 59-70, 2002.
6. M. Grossglauser and D. Tse, “Mobility Increases the Capacity of Ad-Hoc Wireless Networks,”Proc. IEEE INFOCOM,2001.
7. B. Liu, P. Brass, O. Dousse, P. Nain, and D.Towsley, “Mobility Improves Coverage of Sensor Networks,”Proc. Int’l Symp. Mobile Ad Hoc Networking and Computing,2005.
8. W. Zhang, H. Song, S. Zhu, and G. Cao, “Least Privilege and Privilege Deprivation: Towards Tolerating Mobile Sink Compro-mises in Wireless Sensor Networks,”Proc. ACM MobiHoc,2005.
9. F. Li and J. Wu, “Mobility Reduces Uncertainty in MANETs,”Proc. IEEE INFOCOM,2007.
10. W. Zhao, M. Ammar, and E. Zegura, “A Message Ferrying Approach for Data Delivery in Sparse Mobile Ad Hoc Networks,”Proc. MobiHoc,2004.