RESEARCH ARTICLE OPEN ACCESS

# Secured 7 Layer Security Architecture (S7LSA) For Mobile Ad Hoc Network

Manu Srivastava[1], Saurabh Mishra[2], Upendra Kumar Soni[3], Shah Fahad[4]
([1]Assistant Professor, Sagar Group of Institutions, Barabanki, India)
([2, 3, 4] B. Tech (CSE), Sagar Group of Institutions, Barabanki, India)

**Abstract**
Mobile Ad hoc Networks (MANET) constitutes a group of wireless mobile nodes that transmit information without any centralized control. MANETs are infrastructure-less and are dynamic in nature that is why; they require peremptorily new set of networking approach to put through to provide efficacious and successful end-to-end communication. The wireless and distributed nature of MANET poses a great challenge to system security designers. Although security problems in MANET have attracted much attention in the last few years, most research efforts have been focused on specific security areas, such as establishing trust infrastructure, securing routing protocols, or intrusion detection and response, none of the previous work proposes security solutions from a system architectural view. In this paper, we propose seven-layer security architecture for mobile ad hoc networks. A general description of functionalities in each layer is given.
**Keywords:** MANET, SA, S7SLA, Trust

## I. Introduction

A Mobile Ad Hoc Network [1] (MANET) is a collection of wireless mobile nodes constituting an impermanent/unstable network which has no fixed infrastructure where all the nodes configure themselves. In MANETs, changes in network topology may dynamically occur in an unpredictable manner since nodes have liberty to move anywhere arbitrarily. Routing is an important part of MANETs as it gives the better selection of paths. Thus they require efficient routing protocols for providing better communication. For any data communication packets are transmitted in store and forward manner from a source to destination with the help of intermediate nodes.

The nature of ad hoc networks posses a great challenge to system security designers due to the following reasons [2]:

*a.* The wireless network is more susceptible to attacks ranging from passive eavesdropping to active interfering.
*b.* The lack of an online CA or Trusted Third Party adds the difficulty to deploy security mechanisms.
*c.* Mobile devices tend to have limited power consumption and computation capabilities which make it more vulnerable to Denial of Service attacks and incapable to execute computation-heavy algorithms like public key algorithms.
*d.* In MANET, there are more probabilities for trusted node being compromised and then being used by adversary to launch attacks on networks, in another word, we need to consider both insider attacks and outsider attacks in mobile ad hoc networks, in which insider attacks are more difficult to deal with.
*e.* Node mobility enforces frequent networking reconfiguration which creates more chances for attacks, for example, it is difficult to distinguish between stale routing information and faked routing information.

Security has become a primary concern in order to provide protected communication between mobile nodes in a hostile environment and the ultimate goal of the security solutions for MANETs is to provide security services such as Confidentiality, Integrity, Availability, Non-Repudiation and Authentication, Authorization and Anonymity [2].

1***) Confidentiality*** ensures that Secret information or data is never disclosed to unauthorized devices.
2) ***Integrity*** tells that a received message is not corrupted.

3) ***Availability*** permits the survivability of network services despite Denial-of-Service attacks.
4) ***Non-repudiation*** ensures that the sender of a message cannot deny having sent the message.

5) ***Authentication*** enables a node to ensure the identity of the Peer node it is communicating with.

6) ***Authorization*** *i*s a process in which an entity is issued a credential, which specifies the privileges

and permissions it has and cannot be falsified, by the certificate authority.

MANET posses some security challenges which are given below:

1) ***Channel Vulnerability:*** Broadcast Wireless channels allow message Eavesdropping and Injection easily.

2) ***Node Vulnerability:*** Nodes do not reside in physically protected places, thus easily fall under attack.

3) ***Absence of Infrastructure:*** Certification/ Authentication Authorities are absent.

4) ***Dynamically Changing Network Topology*** puts security of routing protocols under threat.

5) ***Power and Computational Limitations*** prevent the use of complex Encryption Algorithms.

## II. Related Work

**T**rust **E**nhanced security **A**rchitecture for **M**ANET [3] (TEAM) has been already proposed for the Mobile Ad Hoc Network, in which a *trust model* is overlaid on other security models such as *key management mechanism*, *secure routing protocol*, and *cooperation model* to enhance the network security. In this architecture, the trust model is designed to capture the evidence of trustworthiness for other nodes from the key management mechanism, secure routing protocol, and cooperation model without introducing further issues such as *honest-elicitation, free-riding,* and *recommender's bias.* The trust model enhances the security decisions of the above security models depending on the predefined policies and collected evidence. The secure routing protocol is utilized to discover secure paths and to protect communications through the secret associations established and maintained by the key management mechanism. In our architecture, the secure routing protocol forwards evidence for fabrication and modification attacks to the trust model, and in return takes advantage of the trust model's feedback to make better routing decisions. Although the key management mechanism does not forward any evidence to the trust model, it relies on the trust model's feedback to dynamically manage the keys. The cooperation model in our architecture differs from related models [4, 5] by defending against both flooding and packet drop attacks. Similar to other security models, it forwards evidence to the trust model, and takes advantage of the trust model's feedback to decide whether to forward a packet on behalf of other nodes. In summary, the proposed ***T**rust **E**nhanced security **A**rchitecture for **M**ANET (TEAM)* extends our previous work, *Trust Integrated Cooperation Architecture* [6] so that it not only assists security models such as key management mechanism, secure routing protocol, and cooperation model to make better decisions, but also enables them to handle the dynamic behaviours of nodes. Hence, ***S**ecure **M**ANET **R**outing with **T**rust **I**ntrigue (SMRTI)* [7, 8], and *fellowship* [9, 10] are chosen for trust and cooperation models respectively.

In this paper, we have proposed the seven layer security solution namely S7SLA using Trust architecture for the Mobile Ad Hoc Network.

## III. S7SLA Model

In this model, we have used the already existing trust model for security of Mobile Ad Hoc networks and further added few layers to design a secured seven layer security architecture for the mobile Ad Hoc networks so that it can be more convenient the to secure the MANETs. This model consist of seven layers namely Co-operation model (fellowship), Routing Security, Key Management Mechanism, Overlay Trust Model, Communication Security, Network Security and End to End Security. The description of these seven layers is given below:

a. **Secured Layer 1-*Co-operation model (fellowship):*** Fellowship model defends against both flooding and packet drop attacks by adopting obligation-based approach, in which nodes are enforced to share the communication channel and forward packets for other nodes in turn to receive similar network services from them.

b. **Secured Layer 2- *Routing Security*:** This implies the security features applied on the routing protocols. In MANET, nodes exchange the information about their knowledge of neighbour node connectivity and construct a view of the network topology so that they can route the data packets to the correct destinations. Every node is required to participate in the routing activity and routing is an important part to keep the network connected.

c. **Secured Layer 3- *Key Management Mechanism*:** Key Management mechanisms are used to discover secure paths and protect subsequent communication.

d. **Secured Layer 4- *Overlay Trust Model*:** This assists the security models in making decisions for the following contexts such as whether to accept or reject a route from a route discovery,

record or ignore a route from a forwarded packet, to forward or discard a packet, to forward a packet for a previous hop, to send a packet to a next-hop, refresh or revoke the key for a node, and which route to choose for the communication.

e. **Secured Layer 5- *Communication Security*:** This refers to security mechanism applied in transmitting data frames in a node to node manner, such as security protocol WEP working in data link layer in OSI or physical protection mechanism like frequency hopping. Security mechanism deployed in this layer may keep data frame from eavesdropping, interception, alteration or dropping from unauthorized party along the route from the source to destination.

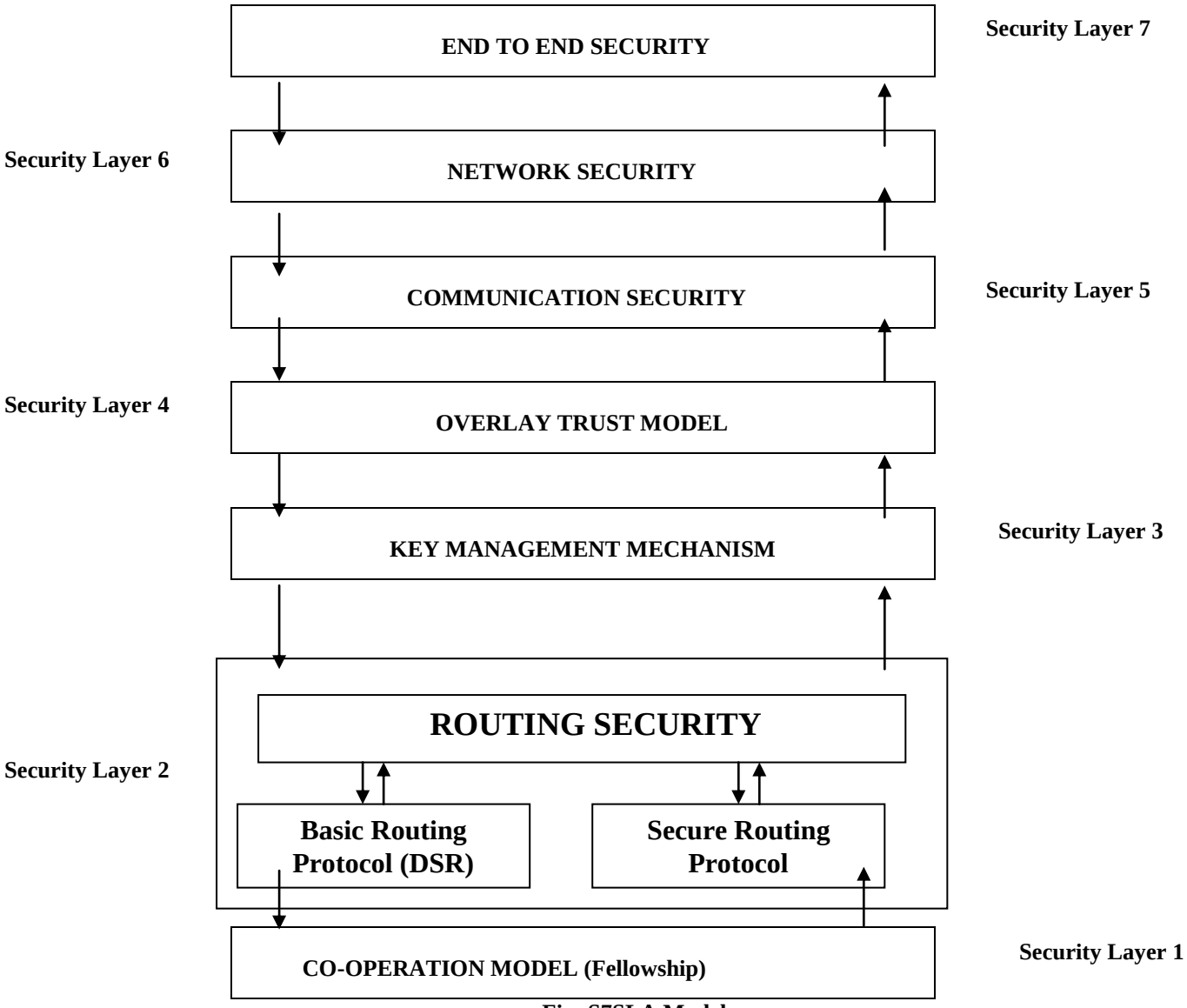


**Fig: S7SLA Model**

f. **Secured Layer 6- *Network Security*:** This refers to the security mechanism used by the network protocols which perform sub-network access from end system to end system. For example we can achieve the security services like peer entity authentication, confidentiality and integrity as the network layer security protocol IPsec provides, another example is SMT mechanism from [8].

g. **Secured Layer 7- *End to End Security*:** This refers end system security such as SSL, SSH and any application specific security protocol. The security protocol in this layer is independent of the underlying networking topology since the related security mechanism

are restricted to only intended parties. The provision of any security service in this layer is highly dependent upon security requirements related to specific applications.

## IV. Conclusion

In this paper, we have taken action towards the security issues Mobile Ad hoc network. We have analyzed the previously existing architectures to enhance the security mechanism applied on them and designed a new secured architecture for the Mobile Ad hoc networks to make it highly secure. We have created the seven layer architecture to formulate the plan making MANET more reliable.

## V. Future Work

In this paper, we have designed the seven layers for providing different security services. We have only given the content conception that how we can secure the MANET in seven different ways. This architecture can be further implemented to apply these security mechanisms on Mobile Ad hoc network.

## References

[1] Charles E. Perkins, "Ad-Hoc Networking", Addision Wesley, 2001.

[2] Ankit Jain, Arnika Jain, Pramod Kumar Sagar, "Various Security Attacks and Trust based Security Architecture for MANET", Global Journal of Computer Science and Technology, Vol. 10, issue 14, November 2010.

[3] Balakrishnan, V. Varadharajan, U. K. Tupakula, and P.Lucs, "Trust Integrated Cooperation Architecture for Mobile Ad-hoc Networks". Proceedings of 4th IEEE International Symposium on Wireless Communication Systems (ISWCS 2007), Trondheim, Norway, 2007.

[4] L. Buttyan and J. Hubaux, "Nuglets: A Virtual Currency to Stimulate Cooperation in Self-organized Ad hoc Networks". Swiss Federal Institute of Technology, Lausanne DSC/2001/001, 2001.

[5] S. Zhong, J. Chen, and Y. R. Yang, "Sprite: A Simple, Cheat-proof, Credit-based System for Mobile Ad-hoc Networks". *INFOCOM 2003*, pp. 1987 - 1997, 2003.

[6] S. Yan Lindsay, Y. Wei, H. Zhu and K. J. R. Liu, "Information Theoretic Framework of Trust Modeling and Evaluation for Ad Hoc Networks". IEEE Journal on Selected Areas in Communications, 24(2), pp. 305-317, 2006

[7] V. Balakrishnan, V. Varadharajan, P. Lucs, and U. K. Tupakula, "Trust Enhanced Secure Mobile Ad hoc Network Routing". Proceedings of 21st IEEE International Conference on Advanced Information Networking and Applications Workshops *(AINAW 2007)*, Canada, pp. 27-33, 2007

[8] V. Balakrishnan, V. Varadharajan, U. K. Tupakula, and P. Lucs, "Trust and Recommendations in Mobile Ad hoc Networks". Proceedings of 3rd International Conference on Networking and Services *(ICNS 2007)*, Athens, Greece, pp. 64-69, 2007.

[9] V. Balakrishnan, and V. Varadharajan, "Fellowship in Mobile Ad hoc Networks". Proceedings of 1st IEEE International Conference on Security and Privacy for Emerging Areas in Communications Networks (Secure Comm. 2005), Athens, Greece, pp. 225-227, 2005.

[10] L Zhou and Z Hass, "Securing Ad hoc networks", IEEE network, vol 13, no. 6, pp 24-30, 1999