Trust Management in Adhoc Networks

M. V. Kulkarni and Shreeji Thankappan
Vishwakarma Institute of Technology, Pune University. E-Mail: shreeji_t@yahoo.com

ABSTRACT
In nature ad-hoc networks makes them vulnerable to attacks in routing to destination. The purpose of securing ad-hoc routing protocols is to protect message to transfer from source to destination through intermediate nodes and to prevent attackers by injecting harmful routing messages into the networks.

In this paper, we present how to prevent an ad-hoc routing protocol by Distributed authentication mechanisms and shared group key by using Hash Message Authentication Code in On Demand Routing Protocol. This mechanism makes trust evaluation to establish a trust relationship between network nodes and gives feedback to adjust it. With this mechanism my protocol exclude the attackers and protect routing message to destination. Using Hash Message Authentication Code with shared group key does message integrity. In Distributed Authentication model, each node maintains Trust Table. In trust table neighbor nodes trust value and trustworthiness are maintain. The trust value of node can be maintained by values which are defined in paper are –1 (distrust), 0 (ignorance), 1(minimal), 2(average), 3(good), 4(complete), where the number is the trust value and the word in “( )” gives the meaning of the value. Trustworthiness of node is defined by > or =2 means “YES” is trustworthy below 2 means “NO” untrustworthy. This model is used to evaluate the trustworthiness of the neighbor nodes. In Hash Message Authentication Code, signature is generated and validate between the nodes to send and receive Route Request between the nodes. It is also to send and receive Route Request between the nodes. It is also used to obtain the message integrity for routing message from source to destination through intermediate nodes. In intermediate nodes, each hop validate the Message Authentication Code by using key, which is shared by next hop is present I path to destination. In ad-hoc network, obtaining the neighbor node is very difficult. Here I implement Hello Protocol, to detect the neighbor node in their coverage area.

CONCLUSION
In this paper, we proposed a secure routing protocol and ad-hoc network with a shared group key as a sole assumption. We developed a Distributed Authentication Model, with which different nodes can authenticate each other.

This protocol can prevent or detect most of the attacks common to ad-hoc routing protocol. Moreover this protocol is capable of discovering multiple routes existed between two nodes and is also appropriate for dynamically changing network topology.

FUTURE SCOPE
Trust value system and trust evaluation functions are important components. But, there are no standards. We plan to optimize them and improve their accuracy in our future work.

REFERENCES