Volume-3, Issue-11, Nov Special Issue -2014 • ISSN No 2277 - 8160

Research Paper | Systems

Secure Communication in Mobile Ad-Hoc Network Using SATEM

S.P.RAMYA	Department of Information Technology, Periyar Maniammai University,Thanjavur
M.MALIK	Department of Information Technology, Periyar Maniammai University,Thanjavur
K.NIVETHA	Department of Software Engineering, Periyar Maniammai University, Thanjavur
V.R.SINDHUJA	Department of Software Engineering, Periyar Maniammai University, Thanjavur

ABSTRACT

To ensure fair and secure communication in Mobile Ad hoc Networks (MANETs), the applications running in these networks must be regulated by proper communication policies. However, enforcing policies in MANETs is challenging because they lack the infrastructure and trusted entities encountered in traditional distributed systems. This project presents the design and implementation of a policy enforcing mechanism based on trusted execution monitor built on top of the Trusted Platform Module. Under this mechanism, each application or protocol has an associated policy. Two instances of an application running on different may engage in communication only if these nodes enforce the same set of policies for both the application and the underlying protocols used by the application. In this way, nodes can form trusted application centric networks. Before allowing a node to join such a network, Satem verifies its trustworthiness of enforcing the required set of Policies. If any of them compromised, Stem disconnects the node from the network. We demonstrate the correctness of our solutions through security, and its low overhead through performance evolution of the applications

KEYWORDS : Security, MANET, distributed systems, Satem, Trusted plateform

1. INTRODUCTION

1.1 Overview

With the maturity of short-range wireless technologies and proliferation of mobile computing devices, building real-life applications over mobile ad hoc networks (MANET) becomes feasible. For instance, two potential applications are traffic monitoring in vehicular networks and peer-to-peer file sharing in ad hoc networks. A key to the success of such applications is a mechanism assuring secure communication and proper collaboration among all participant entities. To achieve this goal, communication policies that govern the interactions between entities must be defined and enforced. For instance, in a traffic Monitoring application, the policy can guarantee that a car always forwards accident alerts to cars coming behind it. Similarly, in a peer-to-peer application, the policy can guarantee that a smart phone can post a query only if it has made several contributions such as publishing files or forwarding other queries. The member nodes in such a network must enforce the policies associated with these applications as well. For instance, a peer-to-peer file sharing application may depend on an on-demand routing protocol. In this case, the mechanism creates a two-tier trusted file sharing network. It first establishes trusted routing tier, and hence a trusted network for routing. Comprising of all the nodes that enforce the routing policy. On top of this tier, it then creates a file sharing tier, enforcing the file sharing policy. In our policy enforcing mechanism, nodes can be members of multiple multi-tier networks simultaneously. For example, let us consider that a vehicular traffic monitoring application uses the same routing algorithm with the file sharing application. Nodes in the aforementioned file sharing network can also establish a traffic monitoring network by creating, on top of the routing tier, a separate trusted tier enforcing the traffic monitoring policy. Two nodes may communicate through an application if and only if they enforce the same application tier policy and all the underlying tier policies.

1.2 AD HOC Network

A wireless ad-hoc network is a decentralized type of wireless network. The network is ad hoc because it does not rely on a preexisting infrastructure, such as routers in wired networks or access points in managed (infrastructure) wireless networks. Instead, each node participates in routing by forwarding data for other nodes, and so the determination of which nodes forward data is made dynamically based on the network connectivity. In addition to the classic routing, ad hoc networks can use flooding for forwarding the data. An ad hoc network typically refers to any set of networks where all devices have equal status on a network and are free to associate with any other ad hoc network devices in link range. Very often, ad hoc network refers to a mode of operation of IEEE 802.11 wireless networks. It also refers to a network device's ability to maintain link status information for any number of devices in a 1 link (aka "hop") range, and thus this is most often a Layer 2 activity. Because this is only a Layer 2 activity, ad hoc networks alone may not support a routeable IP network environment without additional Layer 2 or Layer 3 capabilities. The earliest wireless ad-hoc networks were the "packet radio" networks (PRNETs) from the 1970s, sponsored by DARPA after the ALOHA net project. An ad-hoc network is made up of multiple "nodes" connected by "links".

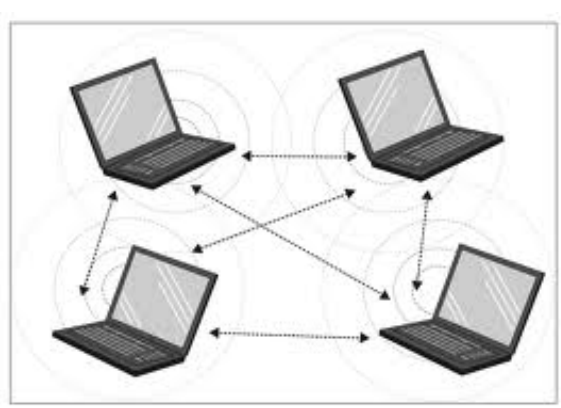


Fig 3.1 Ad hoc network

Links are influenced by the node's resources (e.g. transmitter power, computing power and memory) and by behavioral properties (e.g. reliability), as well as by link properties (e.g. length-of-link and signal loss, interference and noise). Since links can be connected or disconnected at any time, a functioning network must be able to cope with

this dynamic restructuring, preferably in a way that is timely, efficient, reliable, robust and scalable. The network must allow any two nodes to communicate, by relaying the information via other nodes. A "path" is a series of links that connects two nodes. Various routing methods use one or two paths between any two nodes; flooding methods use all or most of the available paths. An ad hoc network is a collection of wireless mobile hosts forming a temporary network without the aid of any established infrastructure or centralized administration. In such an environment, it may be necessary for one mobile host to enlist the aid of other hosts in forwarding a packet to its destination, due to the limited range of each mobile host's wireless transmissions. Mobile ad hoc networks (MANET) do not rely on any fixed infrastructure but communicate in a self-organized way.

Security in MANET is an essential component for basic network functions like packet forwarding and routing: network operation can be easily if countermeasures are not embedded into basic network functions at the early stages of their design. Unlike networks using dedicated nodes to support basic functions like packet forwarding, routing, and network management, in ad hoc networks those functions are carried out by all available nodes. This very difference is at the core of the security problems that are specific to ad hoc networks. As opposed to dedicated nodes of a classical network, the nodes of an ad hoc network cannot be trusted for the correct execution of critical network functions.

1.3 MANET

A mobile ad-hoc network (MANET) is a self-configuring infrastructure less network of mobile devices connected by wireless links. Ad hoc is Latin and means "for this purpose". Each device in a MANET is free to move independently in any direction, and will therefore change its links to other devices frequently. Each must forward traffic unrelated to its own use, and therefore be a router. The primary challenge in building a MANET is equipping each device to continuously maintain the information required to properly route traffic. Such networks may operate by themselves or may be connected to the larger Internet. MANETs are a kind of wireless ad-hoc networks that usually has a routable networking environment on top of a Link Layer ad hoc network. The growth of laptops and 802.11/Wi-Fi wireless networking have made MANETs a popular research topic since the mid 1990s. Many academic papers evaluate protocols and their abilities, assuming varying degrees of mobility within a bounded space, usually with all nodes within a few hops of each other. Different protocols are then evaluated based on measure such as the packet drop rate, the overhead introduced by the routing protocol, end-to-end packet delays, network throughput etc. Mobile Ad-hoc Networks (MANETs) are future wireless networks consisting entirely of mobile nodes that communicate on-the-move without base stations. Nodes in these networks will both generate user and application traffic and carry out network control and routing protocols. Rapidly changing connectivity, network partitions, higher error rates, collision interference, and bandwidth and power constraints together pose new problems in network control particularly in the design of higher level protocols such as routing and in implementing applications with Quality of Service requirements.These networks have no fixed routers, every node could be router. All nodes are capable of movement and can be connected dynamically in arbitrary manner. The responsibilities for organizing and controlling the network are distributed among the terminals themselves. The entire network is mobile, and the individual terminals are allowed to move freely.

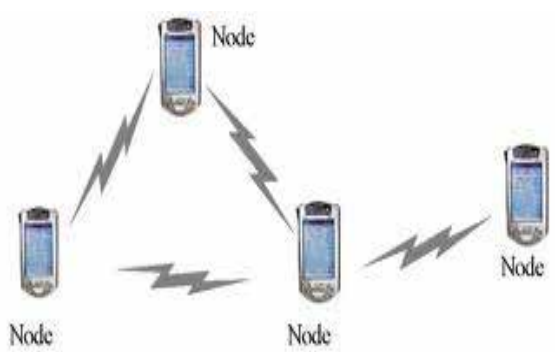


Fig 3.2 Mobile Ad hoc network

In this type of networks, some pairs of terminals may not be able to communicate directly with each other and have to rely on some terminals so that the messages are delivered to their destinations. Such networks are often referred to as multi-hop or store-and forward networks. The nodes of these networks function as routers, which discover and maintain routes to other nodes in the networks. The nodes may be located in or on airplanes, ships, trucks, cars, perhaps even on people or very small devices. Mobile Ad-hoc Networks are supposed to be used for disaster recovery, battlefield communications, and rescue operations when the wired network is not available. It can provide a feasible means for ground communications and information access.

1.4 SATEM

Satem, Service-aware trusted execution monitor to build the trusted policy enforcing mechanism. Originally, we designed and implemented Satem to ensure requesters of a remote network service that the service executes only trusted code. Satem is composed of a trusted agent in the OS kernel of the service platform and a trust evaluator on the user platform. The service provider performs the attestation of the OS kernel (including the trusted agent) through a trusted boot process using the TPM specified by the Trusted Computing Group (TCG). Subsequently, the trusted agent takes advantage of the service execution context to only verify the integrity of the code loaded dynamically by the service. More importantly, it ensures that the service executes only trusted code by protecting the service execution in the OS kernel. Central to Satem is the commitment protocol. Before starting a transaction with a service, requesters ask the trusted agent to provide the integrity measurements of the OS kernel, a system commitment, and a service commitment. The commitments are certificates describing all the code files the kernel and the service may execute in all circumstances (e.g., executables, libraries). The system commitment includes the kernel binary and all the modules it may load. The service commitment includes the entire code stack of the service including the service application binary, shared libraries, other applications. Each piece of software described in the commitments is defined by a combination of its identifier (e.g., name and version) and the SHA1 hashes of all its code files. It is the service provider's responsibility to create appropriate commitments.

The service provider uses static or runtime analysis to determine the code base. Commitments for an application typically include several dozens of code hashes. For example, the system and service commitments altogether for the P2P file sharing application running Mute include 47 code file hashes. The service provider collects the code hashes and generates the commitment certificate as follows, Request code certificates. The service provider requests each vendor to generate a vendor-signed code certificate in the same format as the commitment for its code. The other is Sign the commitment. The requester forwards all the code certificates and the commitment to a third-party trusted Certificate Authority (CA). The CA needs to verify the signatures of all code certificates and compare the code hashes in the commitment against the certificates. The CA signs the commitment if and only if it verifies all code certificates and code hashes in the commitment. Satem only guarantees the integrity and the authenticity of the code, but not its correctness. The requester must have a local trust policy that governs which kernel and services are trusted. It takes two steps to verify whether a service is trusted. First, it authenticates the kernel and service commitment certificates and learns the identities of the kernel, it modules, and the service. Second, it verifies the kernel and the service against the trust policy.

2. EXISTING SYSTEM

Most of the existing policy enforcement solutions have focused on Internet-based systems. Unfortunately, these solutions are not fit for MANET for the following reasons. They enforce policies on trusted "choke points" (e.g., firewall or proxy), which do not exist in MANETs due to the lack of infrastructure.

Furthermore, determining where to place a choke point in a MANET is almost impossible because the paths between nodes change frequently due to mobility. Existing methods aim to protect the servers from unauthorized client accesses. In MANET, this distinction does not exist as every node can be a server and a client at the same time, and no entity can be trusted more than another.

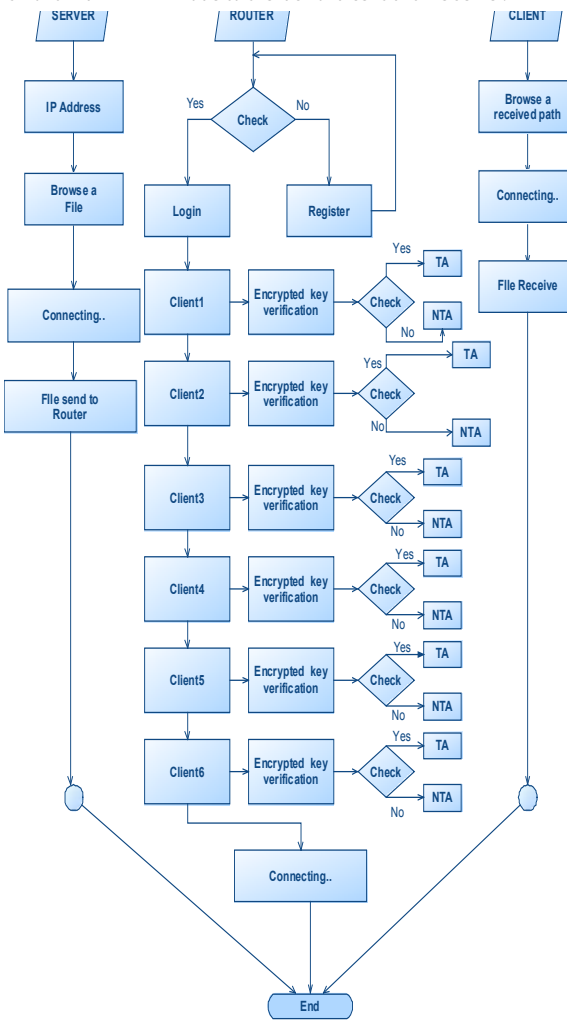
3. PROPOSE SYSTEM

We develop a Satem-based method to implement network access control in ad hoc networks. This project further extends the idea in two fronts.The nodes can now verify the trustworthiness of each other at any layer and for any application rather than just at link layer.A key to the success of such applications is a mechanism assuring secure communication and proper collaboration among all participant entities. To achieve this goal, communication policies that govern the interactions between entities must be defined and enforced. For instance, in a traffic monitoring application, the policy can guarantee that a car always forwards accident alerts to cars coming behind it. Similarly, in a peer-to-peer application, the policy can guarantee that can post a query only if it has made several contributions such as publishing files or forwarding other queries. Different than enforcing policies in the network, another approach is to allow only nodes owned by trusted principals to participate in the network. The method does not address the case of anonymous nodes spontaneously establishing MANETs.

3.1 Proposed Architecture

3.1.1 Secure Routing

A group of nodes supporting Ad hoc On Demand Distance Vector (AODV) routing protocol is considered. AODV is known to be vulnerable attacks, in which an attacker exploits a fast tunnel to attract all network traffic through it. One way to defeat this attack is to implement Packet. The node has to rely on roundtrip delay to estimate the time needed for an AODV message to reach the other. In general, this is nontrivial in MANET due to the lack of a central time server.



3.1 Overall System Architecture

In case of anonymous environment, this becomes more difficult since the two nodes cannot trust each other. The node has to rely on roundtrip delay to estimate the time needed for an AODV message to reach the other. However, this method will accumulate large errors with number of hops and distance between the two nodes increasing. Therefore, the best place to detect the wormhole is on the node that is close to either end of the tunnel. The further away the node is, the less precise the estimate becomes, and the higher false positives and negatives the method incurs. However, this is infeasible since we do not know which node is close to the tunnel and whether this node can be trusted to check the leash. Routing protocols for ad hoc networks are challenging to design: wired networks protocols are not suitable for an environment where node mobility and network topology rapidly change; such protocols also have high communication overhead because they send periodic routing messages even when the network is not changing. So far, researchers in ad hoc networking have studied the routing problem in a non adversarial network setting, assuming a reasonably trusted environment. However, unlike networks using dedicated nodes to support basic functions like packet forwarding, routing, and network management, in ad hoc networks, those functions are carried out by all available nodes. This very difference is at the core of the routing protocols are exposed to many different types of attacks.

4. RESULTS AND DISCUSSION

In Mobile Ad hoc network secure communication has been established using Satem. Satem is developed for establishing a trusted connection. Each node in the network should have the trusted platform. So they can establish a trusted connection between nodes. Client system is used to set the receiving path. Server is used to set the IP address of the destination system. We can select a file and make it to transfer. In router we can set the nodes and we can assign trusted agent, Aodv, file sharing tier in each and every node. If the node all those tiers are in a node, then they are eligible to transfer. After registering the nodes, using encrypted key we can from trusted agent. The file can be transferred to the destination. In future Satem can be added with features so that it can tackle attacks and be more secure. Satem only mitigates the problem in two aspects. Satem may reveal the code that has known buffer overflow vulnerabilities by attesting it to the user. Hence, the user can avoid trusting the vulnerable code.In future satem can be replaced with any other security measures.

5. CONCLUSION

In this paper, we present a mechanism for MANETs to enforce application communication policies. Under this mechanism, nodes supporting the same set of applications and enforcing the same policies construct a trusted multi-tier application-centric network. Client system is used to set the receiving path. In server we set the IP address of the destination system. In router we register the nodes with a username, password, and secret key. Then we login to the node with the help of this username, password. Each node has the capability to accept or reject the AODV tier. After the node accepts the AODV tier, the node automatically generates a encrypted key. With the help of the encrypted key, it checks whether the node has the capability to transfer the file. If the key is incorrect, then file transformation cannot be done. If the key is correct and the nodes are under the trusted agent, then the file is transferred.

REFERENCES

Gang Xu, Cristian Borcea and Liviu Iftode," A Policy Enforcing Mechanism for Trusted Ad Hoc Networks" in IEEE transactions on dependable and secure computing ,vol. 8, no. 3, may-june 2011. | 2. Kannan Govindan, Prasant Mohapatra," Trust Computations and Trust Dynamics in Mobile Adhoc Networks: A Survey" in 2011 IEEE. | | 3. Amit B. Kulkami, Richard Spackmann, Giri Kuthethoor," Self-Organized Management Of Mobile Adhoc Networks" in Proceedings of the 23rd Annual Computer Security Applications Conference, 2008. | | 4.G. Xu, C. Borcea, and L. Iftode, "Trusted application-centric ad-hoc networks," in the Proceedings of the 4th IEEE International Conference on Mobile Ad-hoc Networks and Sensor Systems (MASS 2007), 2007. | | 5.B. Kauer, "Oslo: improving the security of trusted computing," in Proceedings of 16th USENIX Security Symposium on USENIX SecuritySymposium, 2007. | | 6.W. Bagga, S. Crosta, P. Michiardi, and R. Molva, "Establishment of ad-hoc communities through policy-based cryptography," in ElectronicNotes in Theoretical Computer Science, 2007, vol. 171, no. 1, pp. 107–120. | | 7.J. M. McCune, T. Jaeger, S. Berger, R. Caceres, and R. Sailer, "Shamon: A system for distributed mandatory access control," in Proceedings of the 22nd Annual Computer Security Applications Conference, 2006. | | 8.G. Xu, C. Borcea, and L. Iftode, "Satem: A Service-aware Attestation Method Toward Trusted Service Transaction," in the Proceedings of IEEE Symposium on Reliable Distributed Systems (SRDS), October 2006, pp. 321–336. | | 9.E. Shi, A. Perrig, and L. van Doorn, "Bind: A time-of-use attestation service for secure distributed system," in the Proceedings of IEEE Symposium on Security and Privacy, 2005, pp. 154–168. | | 10.L. Zhou and Z. J. Haas, "Securing ad hoc networks," in IEEE Networks, Nov-Dec1999, vol. 13, no. 6, pp. 24–30. |