BSAR Algorithm for Ad-hoc Network Security

Dr Sudhir Dawra
(Associate Professor, Dept. of Computer Science & Engineering)
Ideal Institute of Technology
Ideal Nagar, Ghaziabad- Hapur Road,
Govindpuram Ghaziabad-201301 (U.P)
Telephones: 0120-2767352, 2767351, 2768480 & 81

Abstract

Today, many people carry numerous portable devices, such as laptops, mobile phones, PDAs and mp3 players, for use in their professional and private lives. For the most part, these devices are used separately that is, their applications do not interact. Imagine, however, if they could interact directly: participants at a meeting could share documents or presentations; business cards would automatically find their way into the address register on a laptop and the number register on a mobile phone; as commuters exit a train, their laptops could remain online; likewise, incoming email could now be diverted to their PDAs.
In this paper we outline a security mechanism based on reputation that is used to enforce cooperation among the nodes of a MANET. We then investigate on its robustness using an original approach: we use BSAR model for the interactions between the nodes of the ad hoc network and we focus on the strategy that a node can adopt during the network operation. As a first result, we obtained the guidelines that should be adopted when designing a cooperative security mechanism that enforces mobile nodes cooperation. Furthermore, we were able to show that when no countermeasures are taken against misbehaving nodes, network operation can be heavily jeopardized.

Keywords: Denial of Service Attacks, Simulation, BSAR.

Ad Hoc Network Security

Ad hoc networks are well suited for sensor networks comprised of small wireless electronic devices that can measure and monitor events and physical properties such as temperature, movement, pressure, and location. These sensors can be used to provide visual and audio feedback in environments not easily accessible by humans. Inexpensive wireless sensors can be used to monitor bridges, factories, highways, and buildings, for example, to help improve public safety. Mobile handheld devices such as PDAs and laptops can be used by first responders and today's emerging mobile workforce to easily and quickly set up networks to communicate with their peers.[1] The objective of this research paper is to develop security mechanisms that support secure routing, communication and intrusion detection within small-scale wireless mobile ad-hoc networks (MANET). Additional areas of research include: secure ad hoc communications, secure distributed storage management, distributed trust management, and ad hoc wireless testing tools.

MANET Intrusion Detection Systems

Mobile Ad hoc Networks (MANETs) present a number of unique problems for Intrusion Detection Systems (IDS). [2] Differentiating between malicious network activity and

spurious, but typical, problems associated with an ad hoc networking environment is a challenging task. In an ad hoc network, malicious nodes may enter and leave the immediate radio transmission range at random intervals or may collude with other malicious nodes to disrupt network activity and avoid detection. Malicious nodes may behave maliciously only intermittently, further complicating their detection. A node that sends out false routing information could be the one that has been compromised, or merely one that has a temporarily stale routing table due to volatile physical conditions. [3] Dynamic topologies make it difficult to obtain a global view of the network and any approximation can become quickly outdated. Traffic monitoring in wired networks is usually performed at switches, routers and gateways, but an ad hoc network does not have these types of network elements where the IDS can collect audit data for the entire network. Network traffic can be monitored on a wired network segment, but ad hoc nodes or sensors can only monitor network traffic within its observable radio transmission range.

Secure Routing for MANETs

The majority of the routing protocols proposed in the literature are assuming non-hostile environments. Due to its dynamically changing topology, open environment and lack of centralized security infrastructure, a MANET is extremely vulnerable to malicious node presence and to certain types of attacks that can occur. [4] To address these concerns, several secure routing protocols have been proposed recently: SAODV, Ariadne, SEAD, CSER , SRP, SAAR, BSAR, and SBRP.

Our implementation is based on the Secure Bootstrapping and Routing Protocol proposed in BSAR. Our implementation provides trust establishment on-demand among the nodes that are collaborating to detect malicious activities. A trust relationship is established based on a dynamic evaluation of the sender's *"secure IP"* and of signed evidence. This routing protocol enables the source and destination nodes to establish a secure communication channel between them based on a concept of *"statistically unique and cryptographically verifiable"* (SUCV) identifiers which ensure a secure binding between IP addresses and keys without assuming any trusted certification authority (CA) or key distribution center (KDC). The concept of SUCV is similar to that of Cryptographically Generated Address (CGAs) and it associates a host's IPv6 address with its public key in order for other nodes to verify the ownership of the address.

The Secure Bootstrapping and Routing Protocol runs on Linux-based iPAQs and laptops properly equipped with wireless cards. The implementation has been derived from the HUT-AODV that has been implemented based on the IETF drafts: "Ad-Hoc On-Demand Distance Vector Routing (AODV)" and "Ad-Hoc On-Demand Distance Vector Routing for IP version 6".[5] In our *"SecAODV"* implementation of HUT-AODV we incorporated all secure features described in BSAR and modified the logic of the program as needed.

Ad Hoc Distributed File System

Distributed storage systems are able to share files among peers without the help of a centralized server or centralized location indices. The objective of this paper is to provide secure peer-to-peer file sharing of audit logs and trust credentials in a MANET without any centralized server. The distributed file system is highly survivable, adaptable, and secure.

Ad Hoc Wireless Applications and Testing Tools

During the development of the ad hoc routing protocols we have developed a number of tools

to help test our implementations. These tools will be available for download shortly. These tools include:

- Ipv6Meter is a visual tool for Ipv6 networks that shows that there is reliable connection between a set of three different nodes. Also displays the information about the status of the wireless interface, and draws a graph of the received signal strength vs. time.

- RouteSet is a tool that allows users to quickly setup a star topology network in the ad-hoc environment. [6] This tool is useful to test that all devices will forward IP/IPV6 packets correctly given the routing tables.
- NoComm is a tool that allows the user to artificially disallow communication between any chosen pair of the devices in the ad-hoc network. This tool is useful for debugging routing protocols without a need to physically separate the devices over large distance or attenuate a signal using other means such as metallic foil.
- WirelessParams is an OPIE applet that allows a user to set operating parameters of the CISCO 802.11B card. The parameters that could be set are: SSID, Operating Mode (AdHoc, Infrastructure), the channel number, and the transmit power. This tool also automatically reasserts the chosen SSID, this is done to alleviate the problem with CISCO Aironet cards/ drivers which cause the SSID to be reset.
- Chat is a basic communication program that let's a group of users to exchange messages over an ad-hoc network. Chat supports two modes of operation 'plain text' and 'encrypted'. VPNDaemon is required for encrypted channels. [7]
- VPNDaemon is a glue program that sets up VPN tunnels between every device in the ad-hoc network. It automatically discovers other devices running VPNDaemon and creates connections to them. The devices must have preinstalled X509 certificates, signed by the same central authority. [8]
- Gossip is a distributed directory tool for IPV6 ad-hoc networks. It propagates a table of records describing the devices across the network and maintains its consistency. The records contain name of the devices, its IPV6 address and a public key.
- MiniServer is a small rudimentary file server for IPV6 that uses HHTP like protocol. [9]
- ImageView is a browser to view the images provided by the MiniServer. It uses information collected by the Gossip tool to display the list of hosts, and then it can periodically request an image from the MiniServer on these hosts and display it in the window. Version for the IPAQ is limited to only one full screen image. The version for XWindows can display 6 windows simultaneously.[10]

- MakeMap is a tool that uses information from the Gossip tool to draw the graph of the routing table.

Conclusion

The area of security for ad hoc network has been receiving increasing attention among researchers in recent years. However, little has been done so far in terms of the definition of security requirements specific to ad hoc networks. Security problems in MANET belong to the two fundamental categories: networks with a centralized authority characterizing an a priori trust relationship between the nodes and self-organized networks whereby no a priori trust between the nodes is available.

Countermeasures against node misbehavior in general and denial of service attacks in particular are our very first concern. In this paper we outlined a generic mechanism based

on BSAR to enforce cooperation among the nodes of a MANET and to prevent passive denial of service attacks due to node selfishness.

Bibliography

[1] G. E.Bolton, A. Ockenfels, *ERC: a theory of equity, reciprocity, and competition*. The American Economic Review 2000, 90 166–193.

[2] J.-P. Hubaux, T. Gross, J.-Y. Le Boudec, and M. Vetterli. *Toward self-organized mobile ad hoc networks: The Terminodes Project*. IEEE Communications Magazine, January 2001. IEEE Journal on Selected Areas in Communications, Vol. 17, No. 8, August 1999, pages 1454-1465.

[3] L. Buttyan and J-P. Hubaux. *Enforcing service availability in mobile ad hoc networks*. In proceedings of MobiHOC, 2000.

[4] L.S. Shapley, *Utility comparisons and the theory of games*, Guilbau T (ed.) La decision. Editions du CNRS, Paris, pp. 251-263. Reprinted in: A. Roth (ed.) 1988 The Sahpley Value, Cambridge University Press, Cambridge, pp. 307-319

[5] P. Jacquet, P. Muhlethaler, A. Qayyum, A. Laouiti, L. Viennot, T. Clauseen, "Optimized Link State Routing Protocol draft-ietf-manet-olsr-05.txt", INTERNET-DRAFT, IETF MANET Working Group.

[6] P. Michiardi, R. Molva, *Prevention of Denial of Service Attacks and selfishness in Mobile Ad Hoc Networks*, Institut Eurecom Research Report RR-02-063 - January 2002

[7] P. Michiardi, R. Molva. Simulation-based Analysis of Security Exposures in Mobile Ad Hoc Networks. European Wireless Conference, 2002.

[8] P. Sinha, R. Sivakumar and V. Bharghanan, "CEDAR: a Core-Extraction Distributed Ad-Hoc Routing Algorithm",

[9] S. Marti, T. Giuli, K. Lai, and M. Baker. *Mitigating routing misbehavior in mobile ad hoc networks*. In Proceedings of MOBICOM, 2000.

[10] Tony Larsson, Nicklas Hedman, *Routing Protocols in Wireless Ad hoc Networks - A Simulation Study*, Master Thesis, LuleÅ Tekniska Universities David B. Johnson David A. Maltz, *Dynamic Source Routing in Ad Hoc Wireless Networks*, Mobile Computing, edited by Tomasz Imielinski and Hank Korth, Chapter 5, pages 153-181, Kluwer Academic Publishers, 1996.