Secure Cooperative Routing in Mobile Ad-hoc Networks

Term paper of the 1st semester

C.H.Ngai, Edith

chngai@cse.cuhk.edu.hk
M.Phil student
Department of Computer Science and Engineering
The Chinese University of Hong Kong

Advisor: Prof. Michael R. Lyu

28th November 2002

Abstract

This paper is a survey on the security issues of mobile ad hoc networks. Since mobile ad-hoc networks are getting more and more attentions in recent years, we have great interested in having a survey on the current work in these networks. We found that the most concerning part in using this kind of network is the security issue. Therefore, we focus on the security issues of mobile ad hoc networks and do a survey. At the beginning of the paper, it will give an introduction to the problems on security in mobile ad hoc network that we are facing. Then, it briefly presents what is mobile ad hoc network, its definition, characteristics, applications, standards, and some famous routing protocols. Then, the paper will focus on the security issue and give a detail discussion on the vulnerabilities and the possible attacks that can occur in mobile ad hoc networks. Then, it will move on to the current researches on detection and reaction against malice and selfishness, and on securing ad hoc routing protocols. In the following sections, the most representative papers will be presented. Their approaches, advantages and disadvantages will be listed. Finally, our future plan will be given, and there will be a conclusion.

1 Introduction

As mentioned in the abstract, this is a paper of survey on the security issues of mobile ad hoc networks. Mobile ad hoc networks are a new paradigm of wireless communication for mobile hosts. Hosts are always represented as different nodes in the mobile ad hoc networks. There are a number of differences between mobile ad hoc networks and traditional networks. Ad hoc networks do not rely on any fixed infrastructure. It relies on each other to keep the network connected. Also, the topology of ad hoc networks is dynamically changing and its communication is based on wireless links. Due to the above characteristics, the main challenge in the design of mobile ad hoc networks is their vulnerability to security attacks. That is the reason why we are interested in the security issues on mobile ad hoc networks and it motivates us to do a survey on it.

In this paper, it points out the importance for the security in mobile ad hoc networks. Securing mobile ad hoc networks is particularly difficult with its characteristics. The problem is so broad that there is no way to devise a general solution. It is also clear that different applications will have different security requirements. Among the different aspects of security in wireless ad hoc networks, we divided the difference approaches on securing mobile ad hoc networks into two categories. Among the different approaches, we mainly focus on the cooperative routing in mobile ad hoc networks. In this area, we can divide different mechanisms into two categories. One is the prevention mechanism; another is the detection and discovery mechanism. Details and the recent approaches in these two categories will be presented in later parts of this paper. After reading this paper, an understanding on mobile ad hoc networks, and its security concerns can be obtained. Also, the paper will present the current approaches as a survey, so readers can know what the current trend for researching in this area is.

2 Mobile Ad-Hoc Networks

2.1 Definition

Mobile ad hoc network is a collection of wireless mobile nodes dynamically forming a temporary network without the use of any existing network infrastructure or centralized administration. Due to the limited transmission range of wireless network interfaces, multiple network "hops" may be needed for one node to exchange data with another across the network [1].

2.2 Characteristics

There are a number of characteristics in mobile ad-hoc networks. One of them is that there are dynamic topologies. Nodes are free to move arbitrarily. Thus, the network topology is typically multi-hop, so may change randomly and rapidly at unpredictable times. Another characteristic is bandwidth-constrained. Wireless links will continue to have significantly lower capacity than their hardwired counterparts. Also, there is energy-constrained in the networks. Some or all of the nodes in a mobile ad-hoc network may rely on batteries or other exhaustible means for their energy. Finally, there is limited physical security. Mobile wireless networks are generally more prone to physical security threats than are fixed-cable nets. The increased possibility of eavesdropping, spoofing, and denial-of-service attacks should be carefully considered [2].

2.3 Applications

Examples of potential practical use of mobile ad-hoc networks may be a group of people with laptop computers at a conference that may wish to exchange files and data without mediation of any additional infrastructure in-between. It may be used in home environment for communication between smart household appliances. Ad-hoc networks are suitable to be used in areas where earthquake or other natural disasters have destroyed communication infrastructures. It perfectly satisfies military needs like battlefield survivability, operation without pre-placed infrastructure and connectivity beyond the line of sight. For monitoring and measuring purposes a large number of small computing devices could be spread over a hostile to form a self-sustained ad-hoc network.

Mobile ad-hoc networks have significant advantages above traditional communication networks. For example, use of ad-hoc networks could increase mobility and flexibility, as ad-hoc networks can be brought up and torn down in very short time. Ad-hoc networks could be more economical in some cases as they eliminate fixed infrastructure costs and reduce power consumption at mobile nodes. They are more robust than conventional wireless networks because of their non-hierarchical distributed control and management mechanisms. Also, radio emission levels could be kept at low level because of short communication links (node-to-node instead of node to a central base station). This increases spectrum reuse possibility or possibility of using unlicensed bands. Moreover, communication beyond Line Of Sight (LOS) is possible at high frequencies because of multi-hop support in ad-hoc networks.

Despite the mentioned advantages and potential application possibilities, ad-hoc networks are yet far from being deployed on large-scale commercial basis. Some fundamental ad-hoc networking problems remain unsolved or need optimized solutions. Although various routing protocols are suggested and tested for mobile ad-hoc networks, performance metrics like throughput, delay and protocol overhead in relation to successfully transmitted data need better optimization. This optimization would probably also depend on application type and desire to maximize the throughput or minimize the delay. One single protocol will probably not be able to work efficiently across entire range of design parameters and operating conditions. An additional complexity factor in ad-hoc network design is that different layers of the system are highly interdependent.

2.4 Standards

2.4.1 IEEE 802.11

IEEE 802.11 is a digital wireless data transmission standard in the 2.4 GHz ISM band aimed at providing a wireless LAN between portable computers and between portable computers and a fixed network infrastructure. This standard defines a physical layer and a MAC layer. The most popular technology is the direct sequence spread spectrum and can offer a bit rate of up to 11 Mbps in the 2.4 GHz band, and in the future, up to 54Mbps in the 5GHz band. The basic access method in the IEEE 802.11 MAC protocol is the Distributed Coordination Function which is a Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) MAC protocol. However, the 802.11 standard cannot do multi-hop networking as it is. The development of a number of protocols is required. The maximum data rate of IEEE 802.11 is 11Mbps. Its range is 100 meters [3].

2.4.2 Bluetooth

Bluetooth is a digital wireless data transmission standard operating in the 2.4 GHz Industrial, Scientific, and Medicine (ISM) band aimed at providing a short range wireless link between laptops, cellular phones and other devices. In this band are defines 79 different Radio Frequency (RF) channels that are spaced of 1MHz. The main aim of the Bluetooth Specification is to guarantee the interoperability between different applications that may run over different protocol stacks. However, in order to implement a wireless multi-hop network over Bluetooth, either or both a packet switch layer and a circuit switch layer need to be defines on top of the Bluetooth data link layer protocol. The maximum data rate of Bluetooth is 1Mbps. Its range is 10 meters. Bluetooth has lower power consumption than IEEE 802.11. Also, Bluetooth support both voice and data packet types while IEEE 802.11 just support data packet type [3].

2.5 Routing Protocols

There are a number of routing protocols have been developed for mobile ad hoc networks. They can be divided into two categories, which the table-driven protocols and the source-initiated on-demand protocols. DSDV belongs to the table-driven protocols. The most popular protocols nowadays are the AODV and DSR protocols. Both of them belong to the source-initiated on-demand protocols. We will briefly describe DSDV, AODV and DSR protocols in the following sections.

2.5.1 DSDV

DSDV stands for Destination-Sequenced Distance-Vector Routing. It is a table-driven algorithm based on the classical Bellman-Ford routing mechanism. Table-driven routing protocols attempt to maintain consistent, up-to-date routing information from each node to every other node in the network. These protocols require each node to maintain one or more tables to store routing information, and they respond to changes in network topology by propagating updates throughout the network in order to maintain a consistent network view [4].

2.5.2 AODV

AODV stands for Ad Hoc On-Demand Distance Vector Routing. It builds on the DSDV algorithm. It is an improvement on DSDV because it typically minimizes the number of required broadcasts by creating routes on a demand basis, as opposed to maintaining a complete list of routes as in DSDV algorithm. AODV is classified as a pure on-demand route acquisition system, since nodes that are not on a selected path do not maintain routing information or participate in routing table exchanges. The Figure 1 shows how the AODV route request and route reply message flow[4].

2.5.3 DSR

DSR stands for Dynamic Source Routing. It is an on-demand routing protocol that is based on the concept of source routing Mobile nodes are required to maintain route caches that contain the source routes of which the mobile is aware. Entries in the route cache are continually updated as new routes are learned. The protocol consists of two major phases, which are the route discovery and route maintenance. The route discovery was initiates by broadcasting a route request packet if a node does not have a route to the destination. Route maintenance is accomplished through the use of route error packets and acknowledgements. Route error packets are generated at a node when the data

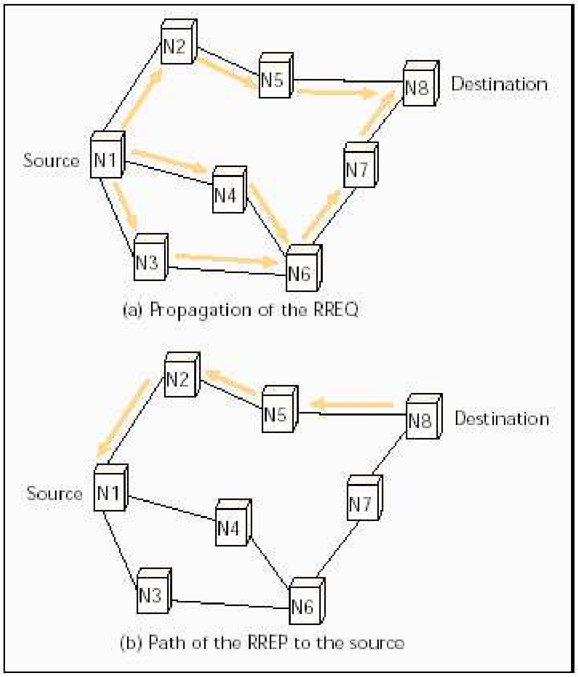
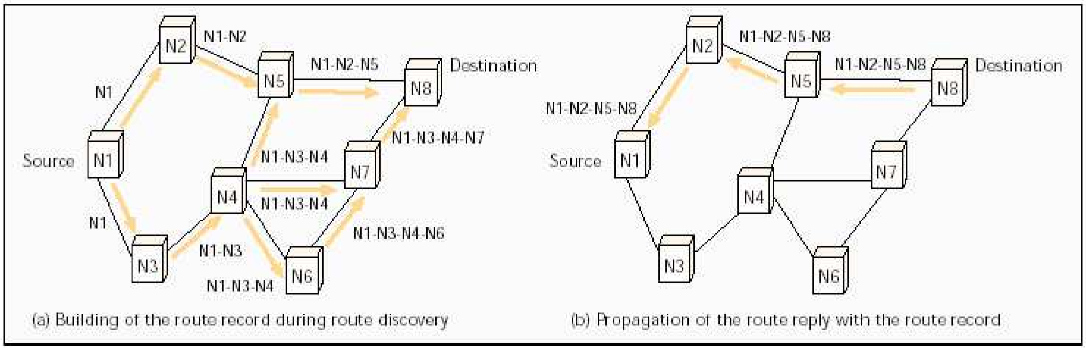


Figure 1: The AODV routing protocol

link layer encounters a fatal transmission problem. The Figure 2 shows how the DSR route request and route reply message flow [4].



(a) Building of the route record during route discovery

(b) Propagation of the route reply with the route record

Figure 2: The DSR routing protocol

3 Security of Mobile Ad Hoc Networks

3.1 Vulnerabilities

Due the characteristics of mobile ad hoc networks that we described in the previous section, there are a number of vulnerabilities of the networks. One characteristic is that mobile ad hoc networks have open medium, and lack of clear line of defence. The use of wireless links renders a wireless ad-hoc network susceptible to attacks ranging from passive eavesdropping to active impersonating, message replay, and message distortion. Active attacks might allow the adversary to delete messages, to inject erroneous messages, to modify messages, to impersonate a node, thus violating availability, integrity, authentication, and non-repudiation. All these mean that a wireless ad-hoc network will not have a clear line of defence, and every node must be prepared for encounters with an adversary directly or indirectly.

Another characteristic is that there is dynamic changing topology. Mobile nodes are autonomous units that are capable of roaming independently. Nodes roaming in a hostile environment with relatively poor physical protection, have non-negligible probability of being compromised. Therefore, not just external attacks should be considered, but attacks launched inside the network by compromised nodes should also be dealt with. It means that nodes with inadequate physical protection are receptive to being captured, compromised, and hijacked. It is easy to attach and hard to detect, so any node in a wireless ad-hoc network must be prepared to operate in a mode that trusts no peer.

Moreover, mobile ad hoc network has decentralized management. There is lack of centralized monitoring and management point. Decision-making in ad-hoc networks is usually decentralized and many ad-hoc network algorithms rely on the cooperative participation of all nodes. Ad hoc network are supposed to operate independently of any fixed infrastructure. This makes the classical security solutions based on certification authorities and on-line servers inapplicable [5].

3.2 Motivation for the Attacks

From the above description, it is clear to notice that mobile ad hoc networks are easy to be attacked. However, it may still be interesting to know what is the motivation for attacking the mobile ad hoc networks. Some reason is that is it possible to gain various advantages by malicious behavior. For example, a node can get better service than cooperating nodes, gain monetary benefits by exploiting incentive measures or trading confidential information, save power by selfish behavior, extract data to get confidential information, and so on [6].

3.3 Types of Attacks

There are many different types of attacks can be occurred in mobile ad hoc networks. One of them is the passive denial-of-service attacks. Under this kind of attacks, the misbehaving providers simply do not perform the requested function. For example, it may not participate to the Route Discovery phase of the protocol. Another type of attack is the active denial-of-service attacks. Under this kind of attacks, the malicious node prevent other providers from serving a request by communicating bogus information on reputation ratings for legitimate nodes, by performing traffic subversion or by using the security mechanism itself causing explicit Denial of Service. There are many other kinds of attacks. Most common attacks are those against routing and forwarding, such as the no forwarding or incorrect forwarding attacks, setting incorrect metrics on route for priority and remaining time in the cache, frequent route updates, and so on.

4 Proposed Researches on Detection and Reaction Against Malice and Selfishness

"Intrusion Detection in Wireless Ad-Hoc Networks", Yongguang Zhang, Wenke Lee, MobiCom 2000.

Background Review

The paper examines the vulnerabilities of a wireless ad-hoc network, and the reason why intrusion detection is needed in ad-hoc network, and why the current methods cannot be applied directly. Finally, it describes the new intrusion detection and response mechanisms that we are developing for wireless ad-hoc networks.

Intrusion was defined as "any set of actions that attempt to compromise the integrity, confidentiality, or availability of a resource". Intrusion prevention techniques, such as encryption and authentication are usually the first line of defence. However, intrusion prevention alone is not sufficient because as systems become ever more complex, while security is still often the after-thought, there are always exploitable weaknesses in the systems.

Research Propose

In this paper, it aims to develop a viable intrusion detection system for wireless ad-hoc networks. It suggests that intrusion detection and response systems should be both distributed and cooperative to suite the needs of wireless ad-hoc networks. In the proposed approach, each node is responsible for detecting signs of intrusion locally an independently, but neighbouring nodes can collaboratively investigate in a broader range.

There are individual IDS agents placed on each and every node. Each IDS agent runs independently and monitors local activities. It detects intrusion from local traces and initiates response. If anomaly is detected in the local data, or if the evidence is inconclusive and a broader search is warranted, neighbouring IDS agents will cooperatively participate in global intrusion detection actions. These individual IDS agent collectively form the IDS system to defend the wireless ad-hoc network. There are 6 components defined in the IDS agent, which are local data collection, local detection engine, local response, global response, cooperative detection engine, and secure communication. The paper also discussed that anomaly detection model should be used in mobile ad-hoc networks [5].

"Mitigating Routing Misbehavior in Mobile Ad Hoc Networks", Sergio Marti, T.J. Giuli, Kevin Lai, and Mary Baker, MobiCom 2000.

Background Review

Ad hoc networks maximize total network throughput by using all available nodes for routing and forwarding. However, a node may misbehave by agreeing to forward packets and then failing to do due to overloaded, selfish, malicious, or broken. An overloaded node lacks the CPU cycles, buffer space or available network bandwidth to forward packets. A selfish node is unwilling to spend battery life, CPU cycles, or available network bandwidth to forward packets not of direct interest to it, even though it expects others to forward packets on its behalf. A malicious node launches a denial of service attack by dropping packets. A broken node might have a software fault that prevents it from forwarding packets. This paper describes two techniques that improve throughput in an ad hoc network in presence of nodes that agree to forward packets but fails to do so.

Research Propose

The paper proposed to install extra facilities in the network to detect and mitigate routing misbehavior. It introduced two extensions to the Dynamic Source Routing algorithm (DSR) to mitigate the effects of routing misbehavior. The two extensions are watchdog and pathrater. There are a few assumptions in this approach. Links between the nodes are bi-directional. Nodes are in promiscuous mode operation. Malicious node does not work in group. Two hops information is required on the packet (DSR can provide it).

There are two extension being added on DSR, which are watchDog and pathrater. A watchdog detects misbehaving nodes by overhearing transmission. Each node was implemented with a watchdog. Each watchdog maintains a buffer of recently sent packets. It compares each overheard packet with the packet in the buffer to see if there is a match. If a packet remained for longer than timeout, increments a failure tally for the node responsible. If the tally exceeds a threshold, the node is determined to be misbehaving and the source will be notified. The advantage of watchdog is that it can detect misbehavior at the forwarding level, and not just the link level. Its disadvantages are that it might not detect a misbehaving node in the presence of ambiguous collisions, receiver collisions, limited transmission power, false misbehavior, collusion, and partial dropping. A pathrater combines knowledge of misbehaving nodes with link reliability data to pick the route most likely to be reliable. Each node was implemented with a pathrater. Each of them maintains a rating fro every other node it knows about in the network. It calculates a path metric by averaging the node ratings in the path. The metric gives a comparison of the overall reliability of different paths. If there are multiple paths to the same destination, it chooses the path with the highest metric.

Simulation was carried out to look for three metrics. They are the network throughput, routing overhead, and effects of false detection. From the analysis of the paper, it shows that the watchdog and the pathrater increases throughput by 17% in network with moderate mobility, while increase ratio of overhead to data transmission from 9% to 17%. Also, it increases throughput by 27% in network with moderate mobility, while increase ratio of overhead to data transmission from 12% to 24% [7].

”Performance Analysis of the CONFIDANT Protocol (Cooperation of Nodes: Fairness In Dynamic Ad-hoc NeTworks)”, Sonja Buchegger, Jean-Yves Le Boudec, Mobihoc, June 2002.

Background Review

The lack of infrastructure and organizational environment of mobile ad-hoc networks offer special opportunities to attackers. Without proper security it is possible to gain various advantages by malicious behavior. Dynamic Source Routing is a protocol developed for routing in mobile ad-hoc networks. There are several routing and forwarding attacks on DSR. The paper aims at protection against a number of types of misbehavior. They are the no forwarding of control messages or data, traffic deviation, route salvaging, lack of error messages, usually frequent route updates, and silent route change.

A method for thwarting attacks is prevention. However, prevention-only strategy only works if the prevention mechanisms are perfect. Otherwise, someone will find out how to get around them. Most of the attacks and vulnerabilities have been the result of bypassing prevention mechanisms. Given this reality, detection and response are essential. In this paper, it proposes a method based on detection of misbehavior, followed by a reaction. It proposes that packets of malicious nodes should, upon detection of the node’s malice, not be forwarded by normally behaving nodes. However, a node was wrongly accused of being malicious or turns out to be repenting offender that is no longer malicious and that has behaved normally for a certain amount of time, re-integration into the network communications should be possible.

Research Propose

The paper proposes the components of CONFIDANT, assumed to be present in every node. CONFIDANT consists of the components, which are the monitor, the reputation system, the path manager, and the trust manager.

The monitor works as a neighborhood watch. The nodes of the neighborhood watch can detect deviations by the next node on the source route by either listening to the transmission of the next node (so-called 'passive acknowledgement') or by observing route protocol behavior. By keeping a copy of a packet while listening to the transmission of the next node, any content change can also be detected. The trust manager consists of an alarm table containing information about received alarms. A trust table managing trust levels for nodes to determine the trustworthiness of an alarm. A friends list containing all friends a node potentially sends alarms to. The reputation system works as a node rating system. The reputation system in this protocol manages a table consisting of entries for nodes and their rating. The rating is changed only when there is sufficient evidence of malicious behavior that is significant for a node has occurred a number of times exceeding a threshold to rule out coincidences. The path manager performs path re-ranking according to security metric, detection of paths containing malicious nodes, action on receiving a request for a route from a malicious node, action on receiving request for a route containing a malicious node in the source route.

Finally, simulation was carried out from the paper. Performance analysis shows a significant improvement in terms of goodput when DSR is fortified with the CONFIDANT protocol extensions. The overhead for this increase is very low. The CONFIDANT protocol is scalable in terms of the total number of nodes in a network and performs well even with a fraction of malicious nodes as high as 60% [8].

"Self-Organised Network-Layer Security in Mobile Ad Hoc Networks", Hao Yang, Xiaoqiao Meng, Songwu Lu, Wise 2002."Hao Yang, Xiaoqiao Meng, Songwu Lu, Wise 2002.

Background Review

Most existing security schemes proposed for mobile ad hoc networks either assume a priori trust or secret association between networking entities, or assume that there is a centralized trusted server in the network. However, the self-organized nature of the ad hoc networks challenges this very basic assumption, and the existence of a centralized server may degrade the effectiveness of the security scheme. AODV has been one of the most popular on-demand routing protocols studied in the research community and IETF. AODV discovers path on-demand, and includes the path maintenance mechanism to handle the dynamics in the network topology. Protecting the network layer in mobile ad hoc network is an important research topic in wireless security. The network-layer vulnerabilities can be divided into two categories, which are the routing updates misbehavior and packet forwarding misbehavior. Routing misbehavior means any action of advertising routing updates that does not follow the specifications of the routing protocol. Packet forwarding misbehavior means any malfunction of the data packet forwarding service as the consequence of an attack. This paper describes a solution to the network-layer security in ad hoc networks in the context of AODV routing protocol.

Research Propose

The self-organised feature of the solution is provided through fully localized design. Each node shares a portion of a global secret, and each node is verified and monitored by its local neighbours collaboratively. In the paper's design, each node is granted temporary admission into the network initially by obtaining a token that will expire soon. Once the token expires, the nodes have to renew it from its local neighbours, which are responsible for monitoring its behaviour collaboratively. The node accumulates its credit as it stays and behaves well in the network. The period of validity of a node's token is proportional to its current credit. This way, a well-behaved node renews its token less and less frequently as time evolves. A malicious node will eventually be detected by its neighbours, its token will be revoked, and it will be denied network access.

The proposed security solution composes of four components. They are the Neighbor Verification, Security Enhanced Routing Protocol, Neighbor Monitoring, and Intrusion Reaction. Neighbor Verification describes how to verify whether each node in the network is legitimate or malicious node. Security Enhanced Routing Protocol explicitly incorporates the security information into the ad hoc routing protocol. Neighbor Monitoring describes how to monitor the behaviour of each node in the network and detect occasional attacks from malicious nodes. Intrusion Reaction describes how to alert the network and isolate the attackers [9].

”Prevention of Denial of Service attacks and Selfishness in Mobile Ad Hoc Networks”, Peitro Michiardi - Rdfik Molva, Research Report, Jan 2002.

Background Review

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 increased sensitivity to nodes misbehaviour in ad hoc networks. If a priori trust relationship exists between the nodes of an ad hoc network, entity authentication can be sufficient to assure the correct execution of critical network functions. A priori trust can only exist in a few special scenarios.

Apart from special cases whereby a priori trust exists in al nodes, the nodes of an ad hoc network cannot be trusted for the correct execution of critical network functions. Node misbehaviour effects these operations may range from simple selfishness or lack of collaboration due to the need for power saving to active attacks aiming at denial of service (DoS) and subversion of traffic. Selfish nodes use the network but do not cooperate, saving battery life for their own hand, aim at damaging other nodes by causing network outage by partitioning while saving battery life is not a priority.

A basic requirement for keeping the network operational is to enforce ad hoc nodes' contribution to network operations and prevent active and passive denial of service attacks. The paper proposes a security mechanism that prevents denial of service attacks enforces nodes cooperation based on a collaborative monitoring technique. The generic mechanism it suggests can be integrated with any network function like packet forwarding, route discovery, network management, and location management.

Research Propose

The paper points out three possible roles that nodes can assume: the requestor, the provider and the peer role. The requestor refers to a node asking for the execution of a function f. The provider refers to any entity supposed to participate to the execution of F. Peers refer to the nodes that are not directly involved in a request or provider exchange but are able to monitor and enforce the fairness for the exchange itself.

The paper proposes a security mechanism that solves the problems due to misbehaving nodes. It incorporates a reputation mechanism that provides an automatic method for the social mechanisms of reputation. There are three types of reputation used in its scheme. Reputation is formed and updated along time through direct observations and through information provided by other members of the community. Also, it takes the stance that reputation is compositional: the overall opinion on an entity that belongs to the community is obtained as a result of the combination of different type of evaluations.

It defines a subjective reputation, an indirect reputation and a functional reputation. Subjective reputation is the reputation that calculated directly from a subject's observation. A subjective reputation at time t from subject s point of view is calculated using a weighted mean of the observations' rating factors, giving more relevance to the past observations. The introduction of indirect reputation adds the possibility for the reputation of a subject being influenced also by information provided by other member of the community. Functional reputation on the other hand, represents the subjective and indirect reputation calculated with respect to different functions f. The paper also defines some validation mechanisms that are used to assure integrity of subjective observations, indirect observations and integrity of explicit DoS messages [10] .

5 Proposed Researches on Securing Ad Hoc Routing Protocols

In mobile ad hoc networks, a lot of research has been devoted to routing algorithms. However, in most cases, the nodes are assumed to be cooperative. Initial work on mitigating routing misbehaviour in mobile ad hoc networks is proposed as mentioned in the previous section. One common method is using some detection component, such as watchdog, to identify the misbehaving nodes. Although the above approach can maintain the total throughput of the network in an acceptable level, the operation of the watchdog required the wireless card works in promiscuous mode [12]. Securing ad hoc networks by using misbehavior detection schemes may not be feasible to detect several kinds of misbehaving, especially because it is very hard to distinguish misbehaving from transmission failures and other kind of failures. Also, it has no real mean to guarantee the integrity and authentication of the routing messages [13].

Recently, there are a number of secure routing protocols proposed. Most of them are built on the existing routing protocols in mobile ad hoc networks, such as the DSDV, DSR and the AODV protocols.

In the paper "Secure Routing for Mobile Ad hoc Networks", it proposed a protocol that can be applied to several existing routing protocols. It presents a route discovery protocol that mitigates the detrimental effects of malicious behaviour, as to provide correct connectivity information. It guarantees that fabricated, compromised, or replayed route replies would either be rejected or never reach back the querying node. Also, the protocol is safeguarded under different types of attack that exploit the routing protocol itself. The requirement of the proposed scheme is the existence of a security association between the node initiating the query and the sought destination. One weak point of this approach is that it does not deal with route error messages. That means, malicious node can forge error messages with other nodes as source [14].

To deal with external attacks, standard schemes such as digital signatures to protect information authenticity and integrity have been considered. The use of a keyed one-way hash function with a windowed sequence number for data integrity in point-to-point communication and the use of digital signature to protect messages sent to multiple destinations [15].

In the paper "Ariadne: A Secure On-Demand Routing Protocol for Ad Hoc Networks", it proposed a protocol called Ariadne. Ariadne was built on DSR and TESLA, and relies on efficient symmetric cryptography. It prevents attackers or compromised nodes from tampering with uncompromised routes consisting of uncompromised nodes, and also prevents a large number of types of Denial-of-Service attacks. One disadvantage of this protocol is that it requires clock synchronization, which is may be an unrealistic requirement for ad hoc networks [16].

In the paper "SEAD: Secure Efficient Distance Vector Routing for Mobile Wireless Ad Hoc Networks", it proposed SEAD as a secure ad hoc network routing protocol based on the design of the Destination-Sequenced Distance-Vector routing protocol (DSDV). In order to support use with nodes of limited CPU processing capability, and to guard against Denial-of-Service (DoS) attacks in which an attacker attempts to cause other nodes to consume excess network bandwidth or processing time, SEAD uses efficient one-way hash functions and do not use asymmetric cryptographic operations in the protocol. This protocol can be used with any suitable authentication and key distribution schemes, but it is not straightforward [17].

In the paper "Securing Ad hoc Routing Protocol", it looks at AODV in detail and develops a security mechanism to protect its routing information. In this paper, it assumes that there is a key management sub-system that makes it possible for each ad hoc node to obtain public keys from the other nodes of the network. Further, each ad hoc node is capable of securely verifying the association between the identity of a given ad hoc node and the public key of that node. Two mechanisms are used to authenticate the non-mutable fields of the messages: digital signature to authenticate the non-mutable fields of the message, and hash chains to secure the hop count information. The hop count is the only mutable information in the messages [13].

6 Future Directions

6.1 Detection and Reaction Against Malice and Selfishness

From the proposed researches described above, more and more attentions have been paid on detecting and isolating misbehaving nodes in the network with cooperation between nodes. All of the researches proposed in this area agree on the importance of cooperation between nodes and the work for monitoring the networks should be distributed and carried out by every node. Generally, a monitoring device will be implemented on every node for detecting misbehaviour, then mechanisms for the exchange of misbehaviour information and isolating the misbehave nodes will be developed.

However, we noticed that most of these protocols only deal with the no forwarding attacks. More different kinds of attacks may be extended to the protocols, for example, forwarding incorrect routing messages, denying execution of particular functions, mismatch between MAC address and the IP address, route diversion, etc. Also, the current protocols cannot deal with attacks made by colluding nodes. Therefore, we think that stronger monitoring or detecting components should be proposed. May be there is a need for combining monitoring between different layers, such as the route message in network layer, the MAC address in the data-link layer, and the functions provided by the nodes in application layers.

Also, the cooperation between different nodes may have many different mechanisms. Generally, the discovery of any malicious nodes will be alerted to normal nodes, and the nodes usually maintain trust ratio (or reputation information) on other nodes in the network. There are different methods for determining when, whom and how to alert the other nodes when some misbehaving nodes are discovered, and different methods are calculating the trust ratio. Methods to efficiently distribute reputation information in order to avoid malicious nodes as early as possible are important and may need further investigation. Apart from the methods to efficiently distribute reputation information, methods for re-integration of an isolated node if the malicious node turns to be a good node again for a long enough period of time should also be developed.

Some protocol, such as the CONFIDANT protocol assumes that nodes are authenticated and that no node can pretend to be another in order to get rid of a bad reputation. Some mechanisms ensure this should be investigated.

6.2 Securing Ad Hoc Routing Protocols

Almost all the proposed ad hoc routing protocols, such as the AODV, DSR, and DSDV, do not have much considering on security. However, there are a lot of vulnerabilities on ad hoc networks as we mentioned before. Secure routing protocol in ad hoc network is becoming a popular topic recently. From the work that had been done in this area previously, it looks that the security needs for ad hoc networks had not been yet satisfied. We believe that there are still lot of space for developing more secure and more efficient routing protocol in ad hoc networks. At least from the previous work, we found different weaknesses in different protocols proposed in securing ad hoc routing protocols. Therefore, one research direction in the future can be keep on developing or improving secure routing protocols in ad hoc networks.

From the investigation on different routing protocols in ad hoc networks, we found the most popular protocols are the AODV and the DSR protocols. They are often been used for research on securing routing protocols. The most significant difference between the AODV and the DSR protocols is their route reply message. In AODV protocol, the route attribute in the route reply message only contains the next hop address. However, the route attribute in the route reply message contains the addresses of all the intermediate nodes on the route in DSR. Therefore, the route reply message of DSR will be longer and less scalable in my point of view. Due to the above reason, we believe that AODV may be the more favourable routing protocol in the future. We are interested in developing a new secure routing protocol in ad hoc network based on the AODV protocol.

To design a secure routing protocol, we need to think of the security protocols and the cryptographic operations will be used in the protocol. Since most routing disruption attacks are caused by malicious injection or altering of routing data. To prevent these kinds of attacks, it is important to keep the integrity and verify the authentication. There are different methods for authentications on data can be used such as the hash functions. Apart from the authentications on data, many secure routing protocols also have an assumption on the presence of key management service underlying the protocols. Therefore, the design of a good key management scheme is also a good research topic. The problem that can be tackled includes the selection of the keys in the protocol, either public or private keys can be chosen with different advantages and disadvantages. Generally, Public Key scheme provides higher level of security guarantee, but with higher complexity. Private Key scheme guarantees lower level of security, but is more efficient. Also, how to set up and distribute the keys to the nodes in the networks is also a problem needs consideration.

Traditional security mechanisms, such as authentication protocols, digital signature, and encryption still play an important role in achieving confidentiality, integrity, authentication, and non-repudiation in ad hoc networks. All these key-based cryptographic schemes demand a key management service. A key management scheme keeps track of bindings between keys and nodes, and assisting the establishment of mutual trust and secure communication between nodes. However, the property of ad hoc network makes it unsuitable to rely on single node as server for key management. To obtain higher level of security, trust should be distributed to all the nodes. For example, the traditional key management scheme uses a single Certification Authority (CA) for key distribution may not be appropriate in mobile ad hoc network. It is because the CA may be easy to be attacked in mobile ad hoc network. If the CA was compromised, it may collapse the entire network as it can sign any attackers into the network using the key of the CA. Therefore, the key management scheme in secure routing protocol on ad hoc network may be a good topic to be considered.

7 Conclusion

In conclusion, a survey on the security issues of mobile ad hoc networks was presented. It looks that the security of mobile ad hoc networks will be given more attentions in the future with the growth of mobile ad hoc networks. Although mobile ad hoc networks can give more mobility and flexibility than traditional communication networks, its lack of infrastructure, dynamic changing topology, and open medium characteristics make it easy to be attacked. It can be noticed that security is an important consideration in the usage of mobile ad hoc networks.

From our survey, there are a number of researches that developed different techniques for the prevention, detection and recovery in the networks against malicious or selfish behaviors. For the prevention mechanisms, most of them are designing more secure routing protocols based on some current developed ad hoc network routing protocols, such as the AODV, DSR, and DSDV routing protocols. However, most of the proposed protocols have different weaknesses and they are unable to deal with different kinds of attacks. Therefore, we think that the area still needs further investigation, so better solution can be obtained.

For the detection and recovery mechanisms, the current approaches use different detection components for detecting the misbehavior of the nodes, and cooperative detection and reputation scheme are always adopted among the neighbors. The misbehavior nodes will be punished or isolated hopefully after they are decided to be untrustworthy. Since the detection and recovery mechanisms have been proposed just in recent two years and their performance still needs further investigation, we think this is another area that can be improved further.

References

[1] David B. Johnson Yih-Chun Hu Jorjeta Jetcheva Josh Broch, David A. Maltz. A performance comparison of multi-hop wireless ad hoc network routing protocols. *MOBICOM*, 1998.

[2] J. Macker S. Corson. Mobile ad hoc networking (manet): Routing protocol performance issues and evaluation considerations. *Network Working Group rfc 2501*, Jan 1999.

[3] Silvia Giordano. Mobile ad-hoc networks. *Handbook of Wireless Networks and Mobile Computing, Wiley*, 2000.

[4] Chai-Keong Toh Elizabeth M. Royer, Santa Babara. A review of current routing protocols for ad hoc mobile wireless networks. *IEEE Personal Communications*, April 1999.

[5] Wenke Lee Yongguang Zhang. Intrusion detection in wireless ad-hoc networks. *Mobicom*, 2000.

[6] Jean-Yves Le Boudec Sonja Buchegger. Nodes bearing grudges: Towards routing security, fairness, and robustness in mobile ad hoc networks. *Workshop on Parallel, Distributed Network-based Processing*, Jan 2002.

[7] Kevin Lai Sergio Marti, T.J. Giuli and Mary Baker. Mitigating routing misbehavior in mobile ad hoc networks. *Mobicom*, 2000.

[8] Jean-Yves Le Boudec Sonja Buchegger. Performance analysis of the confidant protocol (cooperation of nodes: Fairness in dynamic ad-hoc networks). *Mobihoc*, June 2002.

[9] Songwu Lu-Wise 2002."Hao Yang-Xiaoqiao Meng Songwu Lu Hao Yang, Xiaoqiao Meng. Self-organised network-layer security in mobile ad hoc networks. *Wise*, 2002.

[10] Peitro Michiardi Rdfik Molva. Prevention of denial of service attacks and selfishness in mobile ad hoc networks. *Research Report*, Jan 2002.

[11] Peitro Michiardi Rdfik Molva. Making greed work in mobile ad hoc networks. *Research Report RP-02-069*, March 2002.

[12] Srdan Capkun Jean-Pierre Hubaux, Levente Buttyan. The quest for security in mobile ad hoc networks. *Mobihoc*, 2001.

[13] N.Asokan Manel Guerrero Zapata. Securing ad hoc routing protocol. *Wise*, 2002.

[14] Panagiotis Papadimitratos and Zygmunt J. Haas. Secure routing for mobile ad hoc networks. *CNDS*, 2002.

[15] Z.Haas L.Zhou. Securing ad hoc networks. *IEEE Network*, 13(6):24–30, Nov/Dec 1999.

[16] David B. Johnson Yih-Chun Hu, Adrian Perrig. Ariadne: A secure on-demand routing protocol for ad hoc networks. *MobiCom*, 2002.

[17] Adrian Perrig Yih-Chun Hu, David B. Johnson. Sead: Secure efficient distance vector routing for mobile wireless ad hoc network. *WMCSA*, 2002.

[18] Jean-Yves Le Boudec Sonja Buchegger. Cooperative routing in mobile ad-hoc networks: Current efforts against malice and selfishness. 2002.

[19] Jiejun Kong Songwu Lu Lizia Zhung Haiyun Luo, Petros Zerfos. Self-securing ad hoc wireless networks. *ISCC*, 2002.

[20] Haiyun Luo Songwu Lu Lixia Zhang Jiejun Kong, Petros Zerfos. Providing robust and ubiquitous security support for mobile ad-hoc networks. *ICNP*, 2001.