Special Properties of Ad-hoc Wireless Network and Security Models

Han Zhong

Department of Computer Science, University of Auckland

E-mail: hzho023@aucklanduni.ac.nz

Abstract:There are certain amounts of sepecial properties in ad-hoc network. The ad-hoc network in this paper is based on wireless infrasturcture. Because of the limitation of radio range, multi-hop is implemented. The route table need to maintain integrity and confidentility.To cope with diversity of ad-hoc network, different security models are developed. The fundemental of these models is still encryption and decryption, however, the establishment of symmetric/asymmetric keys faces new changelleges.Freely joining or leaving nodes force the authentication more complex.

1. Introduction

Wireless based networks have changed people life greatly, while ad-hoc networks provide people more solutions and convenient due to its special property. Ad-hoc networks are mainly formed by a group of wireless mobile devices. The devices are also called "*nodes*" in ad-hoc network. Ad-hoc networks could be divided into two categories: *mobile ad-hoc networks* (MANETs) and *smart sensor networks*. The typical devices of MANETs are laptops, PDAs, smart mobile phones. MANETs are widely used by public area such as university, airport and hospital. Smart sensor networks could be formed by the small sensors which might be used for data collection, emergency notification. For example, patients' heart rates are sent to doctors' PDA for emergency detection. When people enjoy the benefit of ad-hoc networks, the security also faces challenges according to the special properties.

2. Properties of Ad-hoc Wireless Network

First of all, ad-hoc network is *temporary* network, since each mobile device might leave or join at any time, thus the infrastructure of ad-hoc is dynamical. The devices of ad-hoc wireless network have their own constrains. The communications among devices rely on wireless. Hence, the signal range, also can be addressed to availability, must be taken into count. In reality, a transmitting route is built to enlarge signal range; a packet may be passed one by one along the route to the destination.**[1]** Figure 1 shows how the transmitting route works due to the signal range.

The battery power is limited, i.e. a device may be turned to sleep or shut down anytime. Latency will be caused by the limitation of power supply, since a waiting period may occur when the requested device is asleep. In a previous paper, Frank and Ross mentioned that CPU of portable device is like "peanut" and has very limited computing power. Hence, they must consider about the tradeoff between computing time of encryption algorithm and security.**[2]** However, CPU technology has grown so fast that we do not need to worry too much about the tradeoff due to computing power of portable device. In the other words, we can assume the speed is fair enough to encrypt and decrypt data. Furthermore, latest CPU is more and more energy saves.

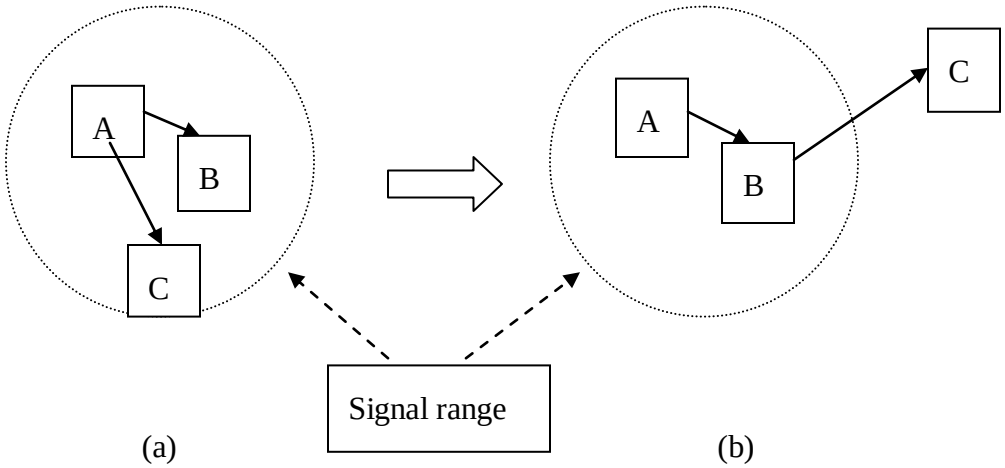

Figure 1: The circle represents the signal range of node A. Initially, nodes A, B, C are in the signal range of node A (a), thus node A can send message directly to node B and C. When node C moves out the range, packets from A to C will go through the rout: A -> B -> C.

Kartin and Guang mentioned that the main distinguish of ad-hoc network is that the networks self-organized. Unlike in WLAN, each nodes is required to be authenticated by authentication server.**[3]**

3. Goals and Risks of Security in Ad-hoc Network

Normally, security goals consist of availability, confidentiality, integrity, authentication, non-repudiation.[4] Due to the special properties of ad-hoc network, Kartin and Gong also more precisely predicted four main security problems[5] except DoS attacks:

(i) Authentication

(ii) Secure key establishment

(iii) Secure routing in multi-hop

(iv) Secure storage of data (key) in the devices

Availability aims to protect network from denial-of-service (DoS) attacks. A DoS attack attempts to use up available bandwidth of networks or resources of nodes. Because ad-hoc network is based on wireless, DoS attacks to ad-hoc network have new method to be carried out. I will discuss about this later.

Confidentiality aims to prevent information disclosure to any unauthorized entity, and this is all about privacy. Hence, confidentiality relies on authentication (i), encryption and non-repudiation. Authentication is very special in ad-hoc network, and I will discuss about it in section 5. The key in (ii) is used to encrypt and decrypt

the information. However, we face a new challenge of establishing keys. The key is also known as session key, which uses symmetric encryption technique.

Integrity aims to protect the content of received packets is correct and never modified by others. Note that the header file might be modified due to transmission route.

Non-repudiation is carried out by tracking and monitoring, and ensures any malicious message is held to be evidence and notify other nodes. Accountability is used by authentication and non-repudiation; however, privacy of user might be disclosed as well. There is paper talked about the balance of privacy and accountability**[6].** When design an infrastructure, balance is a very important issue should be concerned.

Multi-hop is used to enlarge the signal range that is already discussed in section 2. Clearly, it is very important to secure the route from malicious node. For instance, attackers could be benefit of this property that perform sniffer of the communicate channel. Attackers could even hold up all packets passed through them to harm the network. The last one (iv) is not only the security the issue in ad-hoc networks, but also all the other infrastructures.

Furthermore, though the battery power is not an important property to be concerned about due to the improvement of hardware, performance and computing time of encryption is still an important issue. I will discuss about symmetric key later.

4. Denial-of-Service attacks

Denial-of-service attacks can be carried out in different layers of ad-hoc networks. The layers could be categorized into three: physical layer, network layer, application layer. Because ad-hoc network is based on wireless, physical layer DoS, as known as jamming, could be "sending out a strong noise signal in order to prevent packets in the victim network from being received". **[7]** This kind of attack is also called "radio jamming" by Frank and Ross **[2]**. They also said that "radio jamming" is of less relevance to the commercial world. However, their point of view is out of date, since huge amount of commercial activities rely on networks and slower transmission rate or even loss of packets certainly damage the commercial world.

I found that DoS attacks from other layers have little to discuss, if we successfully implement encryption. Because of encryption of packet, i.e. the encryption of both header and content, the attacker cannot request any service from other peers (node in ad-hoc network). However, attackers can resort to physical-layer-based DoS attack that is called "*radio jamming*" mentioned before. A paper focuses on this kind of attack is written by Timothy, Jesse and Amita.**[7]** I found that the DoS attack is more complex in ad-hoc network than others. This is mainly caused by each node of an ad-hoc network may provide services to others. I will not focus on this in this paper; however, I will mainly introduce the authentication and secure communication.

5. Secure Route of Packets

The routing protocol is not fixed in ad-hoc network. Normally, the route of packets is stored in a wireless router or by node itself. The router receives more malicious actions, since it is public and seen by everyone. This security problem does not only occur in ad-hoc network, and I will not focus on this. On the other hand, the route table might be stored in node as private data. Protection of confidentiality is based on authentication which will be introduced below.

5. Security Models

5.1 Basic Model based on Third Trusted Party (TTP)

Lidong and Zygmunt described a design of authentication and key establishment in ad-hoc network. This infrastructure relies on a *key management server* which is used to establish symmetric keys. In this case, both encryption and decryption will use same key. Symmetric key itself will ensure integrity of information.[8] Hence the established key could be also used for authentication.

They also discussed about public/private key infrastructure. In this case, the key management server could be named as *Certificate Authority* (CA). Certainly, we must assume that CA has not been compromised and trusted by all of the nodes. The private key of each node need to be stored securely in both of each node itself and the CA. When a node attempts to communicate with others, device A wants to communicate with device B, for example. Device A need to send request to CA for device B's public key. Then A will have a secure channel to talk with B, and also

the public key could be used to authenticate the identity. Furthermore, nodes have abilities to notify CA to change their key pairs.

5.2 More General Models

It is obvious that this system has its limitation, since whole authentication and key establishment system rely on TTP. If TTP becomes unavailable or is compromised, the whole system will lose security at all. Thus, this infrastructure reduces relaxes and functionalities of ad-hoc network. Another model explained by Kartin and Guang[5] which aims to overcome these shortages, named as KG model in this paper.

Either key management server or CA is of TTP. In KG model, TTP is only required at the stage of initialization of ad-hoc network, and then each node could perform self-organized. Thus TTP can be unavailable and nodes of ad-hoc network could join and leave at any time, and different scenarios are introduced (see figure 2).

AV-1 is another version of Lidong and Zygmunt's design, that is, TTP is always available to nodes. In AV-2, TTP is only available when initializing network and new node joins. In AV-3, TTP is only available during network initialization. In AV-4, TTP is never available. In this case, the design is very challenge that a secure channel need to be implement for node to exchange their keys.

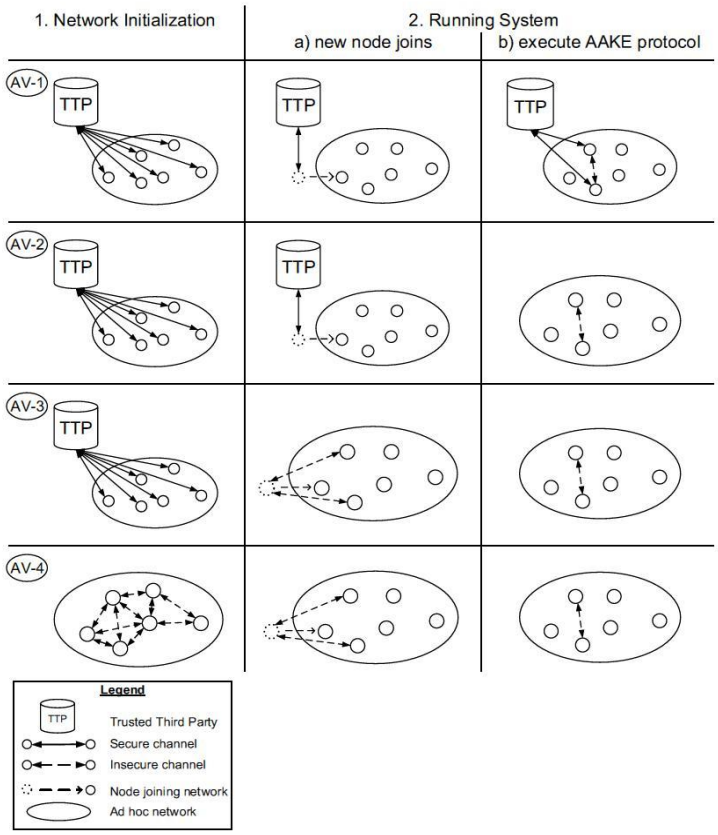

Figure 2: from [5], four scenarios of TTP availabilities. First column (1) represents the situation during network initialization, where (2) represents a new node joining to the networks during running system.

Here, the network initialization is also called *pre-authentication,* as known as *imprinting* in "*resurrecting duckling*" security policy[2]. Kartin and Guang also introduced several security models in details. Overall, the models are based either on symmetric key or asymmetric key. A secure communication channels are required by all of the models. The channels can be divided into two categories: (i) channels for establishing keys and (ii) channels used by nodes to communicate. As

mentioned in section 5.1, a symmetric/public key could be used for authentication, hence (i) is required. While (ii) is required for both confidentiality and integrity.

Some of the models are interesting, like *location-limited* model, for example. In this model, TTP is not regarding with, but only location and trust of each other is focused. This model is only suitable for a small group of devices that can easily perform physical contacts with each others.

6. Conclusion

Security issues of ad-hoc network are special due to the properties discussed before. This paper introduced some current risks of security of ad-hoc network, and also some security models. The basic one in 5.1 is easy to implement with enough resources, however, it will have lager cost and less relax than other models. In reality, ad-hoc network is used by many kinds of applications. According to the properties and aims of each individual application, a all good security model does not exist.

Reference:

[1] A. Kumar, D. Manjunath, J. Kuri, and ScienceDirect (Online service), "Wireless networking," in *The Morgan Kaufmann series in networking* Amsterdam ; Boston: Morgan Kaufmann/Elsevier, 2008, pp. xvii, 427 p.

[2] F. S. a. R. Anderson, "The Resurrecting Duckling: Security Issues for Ad-hoc Wireless Networks." vol. 1796: Springer-Verlag, 1999, pp. 172--194.

[3] Y. Xiao, X. Shen, and D. Du, "Wireless network security," in *Signals and communication technology* New York: Springer, 2007, p. chapter 3.

[4] Z. J. Lidong Zhou Haas, "Securing ad hoc networks," *Network, IEEE*, vol. 13, pp. 24-30, 1999.
doi: 10.1109/65.806983

[5] G. G. Kartrin Hoeper, "Pre-Authentication and Authentication Models in Ad Hoc Networks," in *Signals and Communication Technology*: Springer US, 2007, pp. 65-82.
doi: 10.1007/978-0-387-33112-6

[6] Y. D. Mike Burmester, Rebecca N. Wright, Alec Yasinsac, "Accountable Privacy," in *Security Protocols Workshop, LNCS 3957*, 2004.
doi: 10.1007/11861386_10

[7] X. B. Timothy, E. J. Jesse, and S. Amita, "Jamming and sensing of encrypted wireless ad hoc networks," in *Proceedings of the 7th ACM international symposium on Mobile ad hoc networking and computing* Florence, Italy: ACM, 2006.
doi: http://doi.acm.org/10.1145/1132905.1132919

[8] M. Stamp, "Information security: principles and practice," Hoboken, NJ: Wiley, 2006, pp. 54-55, 76-81.