Security Issues in Monitoring Medical Disease Through Vehicular Ad hoc Network

Priyanka Deodi, Shruti Shrivastava and Mukta Bhatele

Abstract Several diseases and medical conditions require constant monitoring of physiological signals and vital signs on daily bases, such as diabetics, hypertension, etc. In order to make these patients capable of living their daily life, it is necessary to provide a platform and infrastructure that allows the constant collection of physiological data even when the patient is not inside the coverage area. Ad hoc networks are a new wireless networking paradigm for mobile hosts. Unlike traditional mobile wireless networks, ad hoc networks do not rely on any fixed infrastructure. Instead, hosts rely on each other to keep the network connected. The medical, military, tactical, and other security-sensitive operations are still the main applications of ad hoc networks, although there is a trend to adopt ad hoc networks for commercial uses due to their unique properties. One main challenge in design of these networks is their vulnerability to security attacks. In this chapter, we study the threats an ad hoc network faces and the security goals to be achieved. We identify the new challenges and opportunities posed by this new networking environment and explore new approaches to secure its communication.

Keywords Security · Ad hoc network · Routing protocols · Error detection and correction

P. Deodi (✉) · S. Shrivastava · M. Bhatele
Gyan Ganga College of Technology, Jabalpur, India

V. Kumar and M. Bhatele (eds.), *Proceedings of All India Seminar on Biomedical Engineering 2012 (AISOBE 2012)*, Lecture Notes in Bioengineering,
DOI: 10.1007/978-81-322-0970-6_17,

Introduction

Ad hoc networks are a new paradigm of wireless communication for mobile hosts (which we call nodes). In an ad hoc network [1], there is no fixed infrastructure such as base stations or mobile switching centers. Mobile nodes that are within each other's radio range communicate directly via wireless links, while those that are far apart rely on other nodes to relay messages as routers (Fig. 1).

The embedded architecture can be seen in a variety of applications such as invasive sensing, urban sensing, automotive, air and space, and the health care industry. Different platforms have been introduced which can be used to monitor medical data while the patient is out of hospital. These architectures can be used for two classes of applications, some are life critical (ECG Monitoring) and some are not (monitoring the pressure on the feet or the way people are walking after post-knee surgery). Some of the applications that are life critical must have the capability of reporting medical data to physicians with fixed schedules periodically. In addition, these classes of applications must be able to notify the paramedics in case of any emergency to get immediate response. In all the cases when an application intends to transfer data to its appropriate destination, the patient must either be under coverage of a Wi-Fi wireless access point or its on-body terminal must have the capability of using the cellular network. However, in some cases (emergencies, attacks, etc.), neither the Wi-Fi nor the cellular network is available. This fact introduces a major reliability issue regarding the extension of these applications to mobile patients. Vehicles collect data from patients and transfer them to their final destination using ad hoc networks, where each mobile node is a vehicle. The vehicles communicate with each other and with nearby local roadside base stations. Vehicles move in an organized fashion and their range of motion is somehow restricted. For example, they mostly drive in the streets and highways. Moreover, a commuter drives everyday at almost about the same time to work and returns home almost following the same path. Security is an important issue for ad hoc networks, especially for those security-sensitive applications.

Mobile nodes that are within each other's radio range communicate directly via wireless links, while those that are far apart rely on other nodes to relay messages as routers. Node mobility in an ad hoc network causes frequent changes of the network topology. Figure 2 shows such an example: initially, nodes 1 and 4 have a direct link between them. When 4 moves out of 1's radio range, the link is broken. However, the network is still connected, because 1 can reach 4 through 3, 5, and 6.

Ad hoc networks can also be used for emergency, law enforcement, and rescue missions. Since an ad hoc network can be deployed rapidly at relatively low cost, it becomes an attractive option for commercial uses such as sensor networks or virtual classrooms [2, 3].

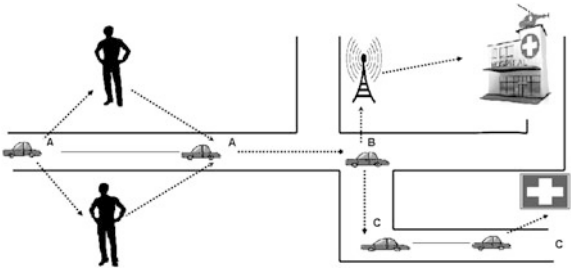

Fig. 1 Vehicles collect data from patients and transfer them to their final destination

Security Goals

To secure an ad hoc network, we consider the following attributes: availability, confidentiality, integrity, authentication, and nonrepudiation. Availability ensures the survivability of network services despite denial of service attacks. A denial of service attack could be launched at any layer of an ad hoc network. On the physical and media access control layers, an adversary could employ jamming to interfere with communication on physical channels. On the network layer, an adversary could disrupt the routing protocol and disconnect the network. On the higher layers, an adversary could bring down high-level services. One such target is the key management service, an essential service for any security framework. Confidentiality ensures that certain information is never disclosed to unauthorized entities. Network transmission of sensitive information, such as strategic or tactical, medical, military information, requires confidentiality. Leakage of such information to enemies could have devastating consequences. Routing information must also remain confidential in certain cases, because the information might be valuable for enemies to identify and to locate their targets in a battlefield. Integrity guarantees that a message being transferred is never corrupted. A message could be corrupted because of benign failures, such as radio propagation impairment, or because of malicious attacks on the network. Authentication enables a node to ensure the identity of the peer node it is communicating with. Without authentication, an adversary could masquerade a node, thus gaining unauthorized access to resource and sensitive information and interfering with the operation of other nodes. Finally, nonrepudiation ensures that the origin of a message cannot deny having sent the message. No repudiation is useful for detection and isolation of compromised nodes. When a node A receives an erroneous message from a node B, nonrepudiation allows A to accuse B using this message and to convince other nodes that B is compromised. There are other security goals (e.g., authorization) that are of concern to certain applications, but we will not pursue these issues in this chapter.

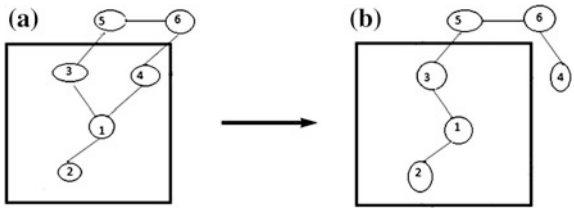

Fig. 2 Topology change in ad hoc networks: nodes 1, 2, 3, 4, 5, and 6 constitute an ad hoc network. The circle represents the radio range of node 1. The network initially has the topology in (**a**). When node 4 moves out of the radio range of 1, the network topology changes to the one in (**b**)

Routing

To achieve availability, routing protocols [4, 5] should be robust against both dynamically changing topology and malicious attacks. Routing protocols proposed for ad hoc networks cope well with the dynamically changing topology [6]. However, none of them, to our knowledge, have accommodated mechanisms to defend against malicious attacks. Routing protocols for ad hoc networks are still under active research. There is no single standard routing protocol. Therefore, we aim to capture the common security threats [7] and to provide guidelines to secure routing protocols. In most routing protocols, routers exchange information on the topology of the network in order to establish routes between nodes. Such information could become a target for malicious adversaries who intend to bring the network down. There are two sources of threats to routing protocols. The first comes from external attackers. By injecting erroneous routing information, replaying old routing information, or distorting routing information, an attacker could successfully partition a network or introduce excessive traffic load into the network by causing retransmission and inefficient routing. The second and also the more severe kind of threats come from compromised nodes, which might advertise incorrect routing information to other nodes. Detection of such incorrect information is difficult: merely requiring routing information to be signed by each node would not work, because compromised nodes are able to generate valid signatures using their private keys. To defend against the first kind of threats, nodes can protect routing information in the same way they protect data traffic, i.e., through the use of cryptographic schemes such as digital signature. However, this defense is ineffective against attacks from compromised servers. Worse yet, as we have argued, we cannot neglect the possibility of nodes being compromised in an ad hoc network. Detection of compromised nodes through routing information is also difficult in an ad hoc network because of its dynamically changing topology: when a piece of routing information is found invalid, the information could be generated by a compromised node, or it could have become invalid as a result of topology changes. It is difficult to distinguish between the two cases. On the other hand, we can exploit certain properties of ad hoc networks to achieve secure routing. Note that routing protocols for ad hoc networks must handle

outdated routing information to accommodate the dynamically changing topology. False routing information generated by compromised nodes could, to some extent, be considered outdated information. As long as there are sufficiently many correct nodes, the routing protocol should be able to find routes that go around these compromised nodes. Such capability of the routing protocols usually relies on the inherent redundancies—multiple, possibly disjoint, routes between nodes—in ad hoc networks. If routing protocols can discover multiple routes (e.g., protocols in ZRP, DSR, TORA, and AODV all can achieve this), nodes can switch to an alternative route when the primary route appears to have failed. Diversity coding takes advantage of multiple paths in an efficient way without message retransmission. The basic idea is to transmit redundant information through additional routes for error detection and correction. For example, if there are n disjoint routes between two nodes, then we can use n−r channels to transmit data and use the other r channels to transmit redundant information. Even if certain routes are compromised, the receiver may still be able to validate messages and to recover messages from errors using the redundant information from the additional r channels. Secure routing in networks such as the Internet has been extensively studied. Many proposed approaches are also applicable to secure routing in ad hoc networks. To deal with external attacks, standard schemes such as digital signatures to protect information authenticity and integrity have been considered. For example, Sirios and Kent propose the use of a keyed one-way hash function with windowed sequence number for data integrity in point-to-point communication and the use of digital signatures to protect messages sent to multiple destinations. Kumar recognizes the problem of compromised routers as a hard problem, but provides no solution. Other works give only partial solutions. The basic idea underlying these solutions is to detect inconsistency using redundant information and to isolate compromised routers. For example, in where methods to secure distance-vector routing protocols are proposed, extra information of a predecessor in a path to a destination is added into each entry in the routing table. Using this piece of information, a path traversal technique (by following the predecessor link) can be used to verify the correctness of a path. Such mechanisms usually come with a high cost and are avoided because routers on networks such as the Internet are usually well protected and rarely compromised.

Conclusion

In this chapter, we have analyzed the security threats an ad hoc network faces and presented the security objectives that need to be achieved. On one hand, the security-sensitive applications of ad hoc networks require high degree of security; on the other hand, ad hoc networks are inherently vulnerable to security attacks. Therefore, security mechanisms are indispensable for ad hoc networks. The idiosyncrasy of ad hoc networks poses both challenges and opportunities for these mechanisms.

References

1. Haas ZJ, Liang B (1999) Ad hoc mobility management using quorum systems. IEEE/ACM Trans Networking 7:2
2. Lee U, Magistretti E, Zhou B, Gerla M, Bellavista P, Corradi A (2006) Mobeyes: smart mobs for urban monitoring with a vehicular sensor network. IEEE Wirel Commun 13(5):52
3. Feldman P (1987) A practical scheme for non-interactive verifiable secret sharing. In: Proceedings of the 28th annual symposium on the foundations of computer science, pp 427–437. IEEE, 12–14 Oct 1987
4. Hauser R, Przygienda T, Tsudik G (1999) Lowering security overhead in link state routing. Comput Netw 31(8):885–894
5. Kumar B (1993) Integration of security in network routing protocols. SIGSAC Rev 11(2):18–25
6. Desmedt Y, Jajodia S (1997) Redistributing secret shares to new access structures and its applications. Technical report ISSE TR-97-01, George Mason University
7. Gong L (1993) Increasing availability and security of an authentication service. IEEE J Sel Areas Commun 11(5):657–662