A MAC layer protocol supporting the application of WSNs in medicine and healthcare domains

Zhongwei Zhang
Department of Mathematics and Computing
Faculty of Sciences
University of Southern Queensland
Toowoomba, QLD 4350
Email: zhongwei@usq.edu.au

Hong Zhou
Department of Electronic Engineering
Faculty of Engineering and Surveying
University of Southern Queensland
Toowoomba, QLD 4350
Email: hong.zhou@usq.edu.au

***Abstract*—Application of Wireless Sensor Networks (WSN) in many fields has achieved a significant advances, many research can be seen in military, industrial control surveillance, and bush fire and wild habitant monitoring, However, it is a bit too early to claim the application of WSN in the domain of Medicine and Healthcare (M&HC) a big success. The major obstacle is the concern raised by the users that how secure the collected data is stored or transmitted over the underlying WSN and how to protect privacy while taking advantage of the technology. In this paper, a sensible solution is proposed to improve the security by augmenting the IEEE 802.15.4 standard with intrusion detection and counterattack mechanism.**

I. Introduction

In the past years, Wireless Sensor Networks (WSN) emerged as a promising technology which has a potential to be adopted in many practical applications [1], [5]. The primary reason is that WSNs can penetrate into areas used to be regarded as dangerous or inaccessible. With advances in sensing technology and wireless networking technology, the cost of making sensor devices is very low, the communication overheads incurred in the data transmitting among the sensor nodes are diminishing considerably. Consequently, the total cost of creating WSNs could be significantly reduced while the capacity of WSNs grows larger than that before. Because of the pervasive nature of sensor devices and flexibility in topology of networks, WSNs hold the promise of facilitating processing large quantity data in realtime.

It envisages that the WSN technology has tremendous potentials of being deployed in the healthcare industries including hospital and nursing homes, that usually involve enormous amount of money and resources, in which many government organisation, private sectors and communities groups invest [4], [5]. Many medical services are vital to human life and the quality of the services are critically detrimental to the wellbeing of society. There are many initiatives and a lot of progress have been made towards the improvement of the quality of healthcare services.

Despite of many progress made mainly on the performance of WSNs and efficient application in data sensitive and real time area, the concerns with the security and privacy have not been given sufficient attention. When it comes to medicine or healthcare domains, the concern with security issue, particular with privacy, becomes immediate and inevasible. There are a number of real life projects and protocols at moment [3], [2]. For example, HealthGear is a Microsoft Research project, it consists of a set of physiological sensors connected

by Bluetooth to a cell phone. In Europe, an initiative called MobiHealth, administrated by European Commission, utilizes UMTS and GRPS networks. Other than that, Imperial College London has a project called Ubimon; while Harvard University in US works on CodeBlue project. In their projects, the IEEE 802.15.6 was standardized for wireless Body Area Networks (WBAN). The MAC layer in IEEE 802.15.6 is design for short range, wireless communication in and around the body area.

Since the application of WSNs in M&HC is likely deployed in hospitals or nursing homes, this is extremely attractive to adversaries which are inquisitive to patients private data such as pregnancy or curious in eavesdropping other peoples health status such as the psychological symptoms and chronic illness. To exploit this vulnerability, adversaries often launch various attacks in the stage of sensor communicating each other or data transmitting between sensor nodes and the gateway station via wireless transmit media. Although the TCP/IP Internet layer architecture is still mentioned while developing the communication protocols for WSN, many research have suggested a cross-layer model probably more appropriate and the only right choice for WSNs, especially in considering the constraints on energy and computational capability. Security threats exist in other places which are located at higher layer in the stack of TCP/IP protocol suites. For instance, Jamming interference is a common threat in physical layer, whilst a popular routing protocol, DSR is susceptible to an attack called neglect and greed.

The reminding of the paper is organized as follows. In Section II, the security issue for general WSN is reviewed, followed by some common security mechanism currently in use. In Section III, we mainly focus on the application of WSNs in medicine and healthcare domains. Apart from the stringent requirements of energy supply, the computational capacity and communication overheads to the sensor nodes, the application of WSNs in this context exerts more strict demand on the protection of data secrecy and private information. To address the security issue, we propose to integrate the intrusion detection strategy with the IEEE 802.11.4 standard in Section IV. In Section V, we focus on a secure MAC layer protocol for the application of WSN in the context of M&HC. Finally in Section VI, we conclude the paper by giving a discussion on the implementation issues, followed by a list of problems for the future.

II. Security in WSN

An application of WSNs usually has tens or hundreds of sensing devices scattered in an area where the targets are confined. Security issues in general application of WSNs are closely linked with these sensor devices. These sensor devices are either to sense environment or track an event happening at a specific location. The sensor devices are of peculiar characteristics such as

- extremely limited in terms of power, computation, and communication
- often deployed in accessible areas
- dynamic ad hoc topology, multicast transmission

The security involves protecting a chain of communication links. The limitation of the WSN devices require that security measures be integrated into every components of the application of WSNs. This requirement makes the WSN subject to the following.

- key establishment and trust setup
- confidentiality and privacy
- integrity and authentication
- availability
- resilience to node compromise
- secure routing
- secure group management
- data aggregation

The existing security protocol and technology that have been used in traditional wireless networks are not necessarily applicable or efficient enough for WSNs. The major reasons behind could be, but not limited to the following.

1) it is impossible to prevent the sensor nodes from being physically accessed by attackers. This indicates an attacker can read sensor nodes' memory or influence the operation of the node software.
2) The constraints regarding memory and computational capabilities are a serious obstacle for implementing the traditional security measures such as cryptographic algorithms.

3) in-network processing is needed to be performed, which means intermediate nodes need to access and modify the information contained in data packets.
4) The limited energy of sensor nodes opens up a particularly attractive line of attacks. That is to say, attackers could have much more energy than the sensor nodes.

The application of WSNs are also very application dependent. It has indicated that the security measures for one application of WSNs could be significantly different than that of other applications of WSNs.

III. Characteristics of Application of WSN

Application of WSN in medicine and healthcare domains has been in demand for long time [1], it has many significance that can provide high quality services in the cost effective way, comparing with traditional healthcare practice. The high quality services mean the services provided by the WSN are more accurate and more prompt. The application of WSN in medicine and healthcare domains focused on monitoring the health status of patients have

(1) The environment of application of WSN is hospital and/or nursing homes. It is open, less , accessible to various kind of persons

(2) The data transmission technology is wireless, which is vulnerable to various attacks.

(3) The objects which the application work on are patients or elderly.

The social implications of the application of WSN include:

- security, privacy and legal issues
- economic and political issues

Security issues are major concern raised by most people. Privacy issue or other social implications are not discussed extensively regarding this field.

For the application of WSNs in the context of M&HC, there are 5 categories of security threats. Each threat requires a solution to meet the security demand.

Category 1: Unauthenticated or unauthorized access. This threat is often dealt with by using random key distribution or public key cryptography to stop adversaries from accessing sensor nodes in the adjacent area.

Category 2: Message disclosure. This threat is very damaging in the sense that the data confidentiality and privacy is breached. A possible countermeasure is to count on the link and network layer encryption or access control.

Category 3: Message modification. The traditional solution to this threat is to use secure hash function or digital signature to protect data integrity and authenticity. We have some reservations on this solution in regarding to the sensor nodes constraints.

Category 4: Denial-of-service (DoS). This threat includes many types of attacks, mainly related to the availability. They are all called DoS attacks [6], they could be adversaries attempt to disrupt, subvert, or destroy a network, could be hardware failures and software bugs, even resource exhaustion. An intrusion detection mechanism is probably a sensible solution.

Category 5: Intrusion. This threat is kind of high level attacks. Possible security solution to this type of attacks include secure group communication and intrusion detection.

In this paper, we actually describe one solution based on intrusion detection. In Section IV and V, we will detail the MAC layer protocol in IEEE 802.15.4 with RTS/CTS mechanism added and a method of detecting or determining one of three types of possible intrusion.

IV. MAC Layer Protocol for WSN-M&HC

IEEE 802.15.4 standard was initially designed for the application of WSN in home automation, home networking, connecting devices to a PC, home security and so on. It covers the physical layer and the MAC layer of a low-rate wireless network. The physical layer offers bitrate of 20 Kbps using a single channel in frequency range 868-868.6 MHz. If it uses 10 channels in the range between 905-928MHz, the physical layer protocol can offers a bitrate up to 40 Kbps. Actually it is possible for the physical layer to offer a bitrate of 250 Kbps when 16 channels in the 2.4 GHz ISM band between 2.4-2.485 GHz with 5 MHz spacing between the center frequencies.

The MAC layer protocol of IEEE 802.15.4 combines both schedule based as well as contention based schemes. The current contention-based MAC protocol is pretty good in achieving the performance

and efficiency. This MAC layer protocol is called slotted CSMA-CA protocol. We can easily realize that the slotted CSMA-CA protocol has no provision against hidden-terminal problem due to no RTS/CTS handshake, but it uses random delays to reduce the probability of collisions. Consequently, it is desirable to add the RTS/CTS mechanism to the slotted CSMA-CA protocol.

The slotted CSMA-CA protocol is mainly to arbitrate sensor nodes to get access to the shared transmission channel. Figure IV depicts the algorithm used by the slotted CSMA-CA protocol.

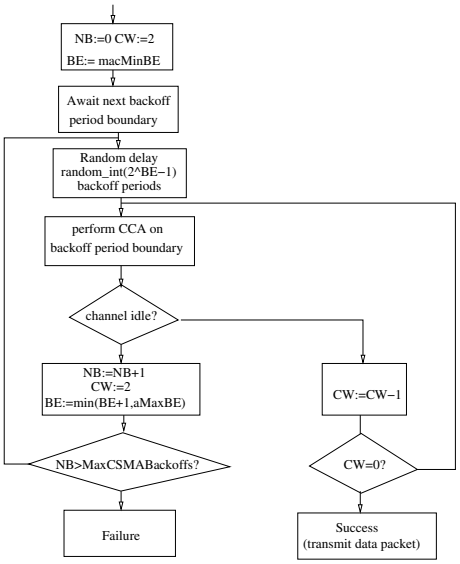

Fig. 1. Slotted CSMA-CA algorithm

V. Secure Slotted MAC Protocol

With the slotted MAC layer protocol, the application of WSNs in the context of M&HC is susceptible to attacks by malicious intruders. Traditional security mechanism, such as authentication protocols, digital signature, and encryption are not sufficient to prevent the underlying WSN being attacked. For instance, the Slotted MAC protocol with RTS/CTS mechanism are vulnerable to collision attack; that is adversaries lunch attack through sending out some packets to disrupt the data packets sending process without being prevented during the exchanging period of RTS and CTS packets. Secondly, we could find out that the slotted MAC protocol is vulnerable to a kind of attack — unfairness attack. This attack is due to the characteristics of the RTS/CTS-based MAC protocols, namely each node has the same priority to get the common channel and if one node gets hold of the channel, all other nodes have to wait for a random length time before trying to transmit packets. Adversaries could send out packets just waiting for a very short or without waiting at all.

To improve the safety of the slotted MAC layer plus the RTS/CTS mechanism, two modules are added to each node and the modules will be executed automatically all the time. The two modules are intrusion detection and defense module. The intrusion detection module meant to determine whether an intrusion has occurred, and it will trigger the defense module to stop transmission or receiving at this time. The approach of stopping transmitting or receiving is virtually to force the node switch to sleep mode for a period of time.

Hence the problem has now turned into as rightfully detection of intrusion by a node. The detection of intrusion is based on the statistics of four indicators.

- Collision Ration (R_c): R_c is the collision times detected by a node per second.
- Probability of Data Packet Successful Transmission (P_{st}): A successful transmission is defined as a correct sending and receiving process of data packet. P_{st} is the ratio of the number of successful data packets transmitted to the total number of data packet transmitted.
- Data Packet's Waiting-Time (T_w): T_w is the time of data packet in MAC layer buffer waiting for transmission.
- RTS Packets Arrival ratio (R_{RTS}): R_{RTS} is the number of RTS packets received successfully by a node per second.

The intrusion detection module will collect the statistics of all four indicators, and estimate the intrusion probabilities for each of them. The probabilities of intrusion are estimated by through a decision function, which is represented in Eq (1)

$$y(x) = \frac{1}{1 + exp[-A \times (x - C)]} \qquad (1)$$

Where the decision function $y(x)$ is representing a curve with two parameters: 'A' and 'C'. They determine the slop and the center of curve, respectively. The shape of the curve is adjustable and will be adjusted by changing the parameters 'A' and 'C'.

The intrusion probabilities of three types of attacks are defined as follows:

- Probability of collision attack (P_c): P_c is the probability of collision attack found. It directly relates to R_c ;
- Probability of exhaustion attack (P_e): P_e is the probability of collision attack found. It directly relates to R_{RTS} ;
- Probability of unfairness attack (P_u): P_u is the probability of unfairness attack found. It directly relates to T_w ;

The probability of one kind of intrusion is determined by comparing the combined value of P_{st} with one of other three intrusion indicators with a threshold. For example, to detect a collision attack, we would compare the combined value of P_t and P_c with a threshold P_{th} , ie.

For the detection of collision attack, Eq(2) is sued as a criteria.

$$\alpha P_t + \beta P_e > P_{th} \tag{2}$$

where $P_t = \frac{1}{1+exp[-A\times(P_{st}-C)]}$ and $P_e = \frac{1}{1+exp[-A\times(P_{RTS}-C)]}$

Similarly for the detection of unfairness attacks, Eq(3) is the one we have to use.

$$\alpha P_t + \beta P_u > P_{th} \tag{3}$$

where P_t is the same as above, and $P_u = \frac{1}{1+exp[-A\times(T_w-C)]}$ and for the detection of exhaustion attacks, we take Eq(4) as a criteria.

$$\alpha P_t + \beta P_e > P_{th} \tag{4}$$

where P_t is the same as above, and $P_e = \frac{1}{1+exp[-A\times(P_{RST}-C)]}$

Note that α, β are the weights between 0 and 1.

It is quite obvious that in sleep mode or idle mode, the R_c , T_w , R_{RTS} are much lower than those in transmitting mode or receiving mode. Therefore the decision function defined in Eq.(1) should be adaptive. That means the parameter 'A' and 'C' in (1) should be varying in different modes.

There are many approaches to determine 'A' and 'C'. In our study, we may adopt an intelligent approach based on fuzzy logic.

VI. Conclusion

Wireless sensor networks (WSNs) hold the promise of ubiquitous computing and the application of WSNs can be seen in military, environment monitoring, safety-critical or domestic infrastructures surveillance. This paper has investigated two important issues: security in wireless sensor networks, particular in the application of WSNs in the context of M&HC.

The slotted CSMA-CA protocol has been adopted as the MAC layer protocol in IEEE 802.15.4 standard by many WSNs. Without the RCS/TCS mechanism, the protocol is vulnerable to many attacks which are very common on the application of WSNs in medicine and healthcare domain, we proposed to add the RCS/CTS mechanism onto the slotted CSMA-CA protocol. In addition, we further integrate the MAC layer protocol with the intrusion detection technology which has defined three criteria for determining an appropriate attack, and react on it accordingly.

In the future, we intend to implement the modified MAC layer protocol combined with the proposed intrusion detection strategy on the application of WSNs satisfying special requirements from hospitals or nursing homes. The implementation might be begun on NS2 or a real wireless sensor network in our sensor network laboratory.

References

[1] Korhonen, Ilkka and Bardram, Jakob B. *Guest editorial introduction to the special section on pervasive healthcare*. IEEE Transaction on Information Technology in Biomedicine, vol 8, no.3, 2004, pp229-234.

[2] Moshaddique Al Ameen and Jingwei Liu and Kyungsup Kwak, *Security and Privacy Issues in Wireless Sensor Networks for Healthcare Applications*, Springer, 12 March 2010.

[3] H S Ng, and M L Sim and C M Tan: *Security issues of wireless sensor networks in healthcare applications*, BT Technology Journal, vol 24, no.2, April 2006, pp138-144.

[4] Farooq Anjum and Saswati Sarkar: *Security in Sensor Networks*, Mobile Wireless and Sensor Networks: Technology, Applications, and Future Directions. (eds. Rajeev Soorey et al), 2006, pp283-307.

[5] Holger Karl and Andreas Willig: *Protocols and Architectures for Wireless Sensor Networks*, John Wiley & Sons. 2005.

[6] Anthong D. Wood and John A. Stankovic: *Denial of Services in Sensor Networks*, IEEE Computer, 2002. pp54-62.