Signature-based intrusion detection in healthcare wireless sensor networks implemented over IEEE 802.15.4 beacon enabled clusters

Jelena Mišić, Fereshteh Amini, Moazzam Khan,

University of Manitoba, Winnipeg, Manitoba, Canada

Keywords: Security in wireless sensor networks, security attacks, intrusion detection, healthcare sensor networks, personal area networks, IEEE Std 802.15.4, CSMA-CA

Definition: We analyze possible security attacks to the personal WSN carried on the patient's body and its close vicinity. We assume that WSN is implemented using 802.15.4 beacon enabled technology with a secure sensing, location and power management blocks based on the ZigBee specification and built on top of 802.15.4 link layer. We present networking and security issues which can be used as a basis for security attacks.

1 Introduction

Healthcare is an important area for deployment of wireless sensor networks (WSN). The IEEE 1073 Medical Device Communications standards organization is currently in the process of developing the specifications for wireless interface communications. The main objective for this effort is to develop universal and interoperable devices for medical equipment which are transparent to the user and easily re-configurable. The group has recognized that developing new wireless technologies is not an option and is looking instead in deployment of existing wireless technologies belonging to IEEE 802 family in the healthcare applications.

In order to penetrate the market with cost-effective solutions for healthcare WSNs we need standardized low-cost, low-power and short-range communication Low Rate Wireless Personal Area Network (LR-WPAN) technology. Important candidate for the application in this area is IEEE 802.15.4 standard [4]. From the aspect of patient's privacy, it is necessary that each patient carries his/her own body WSN using lightweight devices. Health data collected from patient's body have to be gathered at the device possessed by the patient and further communicated to the information system belonging to the healthcare institution. Such data have to be protected from the aspects of confidentiality and integrity. Therefore patient's health data collecting device also has the function of Patient Security Processor (PSP). Beacon enabled mode of IEEE 802.15.4 suits this architecture since it supports many sensing nodes communicating directly with cluster coordinator which in our case has the function of the data collecting device, bridge towards the healthcare information system and PSP.

The 802.15.4 specification outlines some basic security services at the data link layer that can be combined with advanced techniques at the upper layers to implement a comprehensive security solution. For example, the recent ZigBee specification [17] implements a number of protocols—including security-related ones—that can be deployed in an 802.15.4 network. Given that the 802.15.4 devices are typically severely constrained in terms of their communication and computational resources, the implementation of such solutions is likely to impose a significant performance overhead. For the reason of cost effectiveness we assume that Symmetric-Key Key Establishment (SKKE) [17] is implemented over the body WSN, which in turn is a IEEE 802.15.4 sensor cluster operating in beacon-enabled, slotted CSMA-CA mode. In this Chapter we analyze the possible security attacks on the patient's body WSN.

The Chapter is organized as follows. In Section 2 we present basics of security in Wireless Sensor Networks while in Section 3 we discuss the intrusion detection techniques in networks. In Section 4 we present the architecture of the healthcare network including patient's body WSNs. Section 5 gives a brief overview of the operation of 802.15.4-compliant networks with star topology in the beacon-enabled, slotted CSMA-CA mode, followed by a review of basic security mechanisms provided for by the standard. As the 802.15.4 specification does not prescribe any particular key management approach, we will make use of the SKKE mechanism presented in Section 6. Section 7 discusses the possible attacks, while Section 8 concludes the Chapter.

2 Security in wireless sensor networks

The security architecture of WSNs is different from other kinds of networks, due to its special characteristics. First, we have to make sensor networks economically viable as sensor devices are limited in their energy, computation, and communication capabilities. Second, unlike traditional networks, sensors are often deployed in inaccessible area, presenting the added

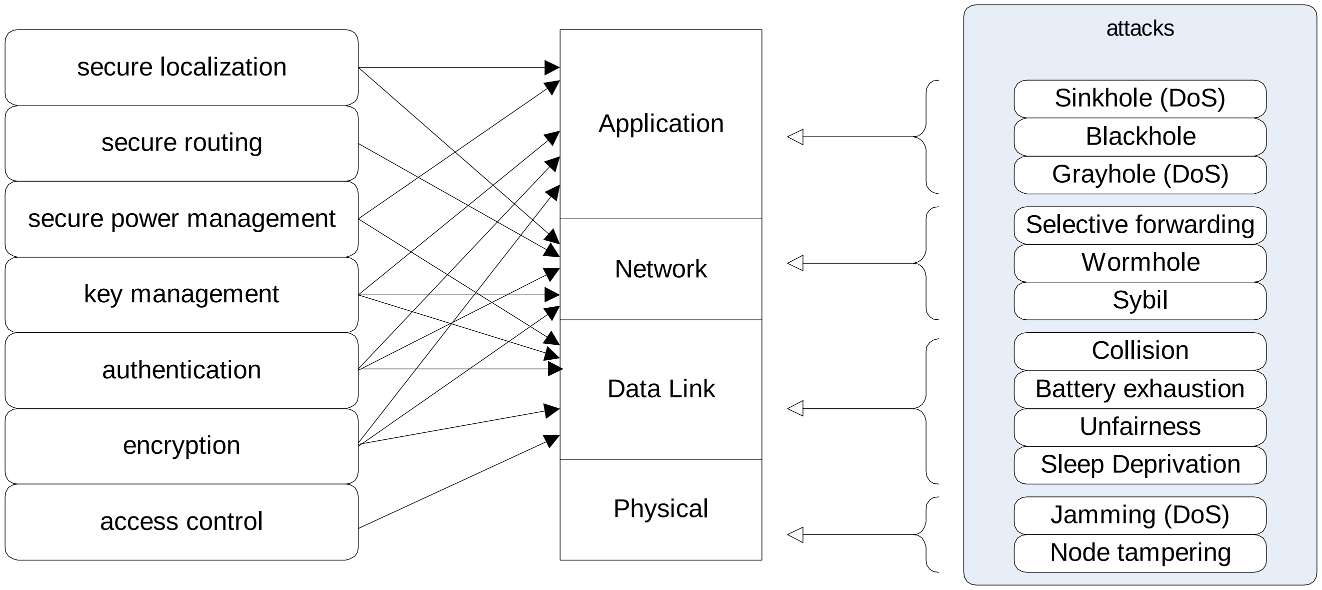


Figure 1. The anatomy of security in Wireless Sensor Network.

risk of physical attack. Third, sensor networks interact closely with their physical environments and with people, posing new security problems. Consequently, existing security mechanisms are inadequate, and new ideas are needed.

Security of a network is determined by the security over all layers. For example, confidentiality, integrity, and availability typically address security of the link layer. Referring to Figure 1, we note that securing the link layer provides a certain level of security to the layers above; however, it does not address security problems in the physical layer below, most notably jamming. In general, an insecure physical layer may practically render the entire network insecure, even if the layers above are secure. This is especially true in the sensor network environment since basic wireless communication is inherently not secure. In the rest of this section, we will study some security considerations for WSN followed by security consideration for IEEE 802.15.4 network will be presented.

2.1 Security View through basic security services

Authentication is necessary to enable sensor nodes to detect maliciously injected or spoofed packets. It enables a node to verify the origin of a packet and ensure data integrity. Almost all applications require data authentication. In military and safety-critical applications and even in civilian applications such as office/home applications, where we expect a relatively secure environment, the adversary has clear incentives to inject false data reports or malicious routing information. Although authentication tries to prevent outsiders from injecting or spoofing packets, it does not solve the problem of compromised nodes. Since a compromised node has the secret keys of a legitimate node, it can authenticate itself to the network. However, we may be able to use intrusion detection techniques to find the compromised nodes and revoke their cryptographic keys network-wide.

Ensuring the secrecy also known as confidentiality of sensed data is important for protecting data from eavesdroppers. We can use standard encryption functions and a shared secret key between the communicating parties to achieve secrecy. However, encryption itself is not sufficient for protecting the privacy of data, as an eavesdropper can perform traffic analysis on the overheard cipher text, and this can release sensitive information about the data. In addition to encryption, privacy of sensed data also needs to be enforced through access control policies at the base station to prevent misuse of information.

Providing availability requires that the sensor network be functional throughout its lifetime. Denial of Service (DoS) attacks result in a loss of availability. In practice, loss of availability may have serious impacts. In a manufacturing monitoring application, loss of availability may cause failure to detect a potential accident and result in financial loss; in a battlefield surveillance application, loss of availability may open a back door for enemy invasion. Various attacks can compromise the availability of the sensor network. When considering availability in sensor networks, it is important to achieve graceful degradation in the presence of node compromise or benign node failures.

Service integrity is another security requirement. Above the networking layer, the sensor network usually implements several application-level services. Important components of integrity are origin authenticity and data authenticity.

2.2 Security View through Secure Blocks of Protocol Layers

To provide previously discussed security services, WSNs utilize several security mechanisms. The higher blocks in Figure 1 use the functionalities presented by the lower blocks. We can say that the two block sections are orthogonally related. Secure Location, which is a mechanism applied through application and network layers of protocol stack, will need to have authentication, encryption and access control to provide a secure location service on top of other services. The same goes for Secure Routing and Secure Power Management. Secure routing requires services from lower blocks such as authentication and access control since the integrity of routing request/reply and neighborhood information must be protected. Power management service grantees required event sensing reliability and network lifetime. Integrity of this service is important. Location service provides geographical location of the node which accompanies report of data. It is necessary to provide integrity of this service.

3 Intrusion detection

Since network-based computer systems have come to be used in various facets of our lives, they have become the targets of intruders. An adversarys malicious attack may violate integrity, availability and confidentiality of an information system or its data. Intrusion prevention techniques, such as encryption and authentication (e.g., using passwords and biometrics) which are the first line of defense, are usually not sufficient because of complexity of network systems. On the other hand preventing attacks from insider nodes in WSN is very difficult. Therefore intrusion detection mechanisms are necessary to detect these malicious nodes. Intrusion detection and response, provide second line of defense. Given that new vulnerabilities will be discovered and the fact that our adversaries will continue to invent new attack methods, specially for a relatively new technology such as WSN, we have to use effective detection approaches. An Intrusion Detection System (IDS) may be classified based on the detection technique [1]:

- A potential intrusion is reported by Misuse or Signature-based detection if a sequence of events within a system matches a set of known security policy violations. In order to detect an intrusion by Misuse model a knowledge of potential vulnerabilities of the system should be available. The intrusion detection system then applies this rule set to the sequences of data to determine a possible intrusion. This technique may exhibit low false positives, but does not perform well at detecting previously unknown attacks. Subhadrabandhu et al. [15] present a robust intrusion detection using misuse detection technique. Anjum et al. [2] deal with the ability of various routing protocols to facilitate intrusion detection techniques when the attack signatures are completely known in network.

- Anomaly detection uses a set of expected values to compare with systems behavior. If the computed statistics do not match the expected values, an anomaly is reported. Anomaly-based detection defines a profile of normal behavior and classifies any deviation of that profile as an intrusion. The normal profile is updated as the system learns the subjects behavior. This technique may detect previously unknown attacks but may exhibit high false positives. Zhang et al. [16], present an anomaly detection model. They use trace data which describes the normal updates of routing information Since, the main concern is that false routing will be used by other nodes. The generated trace data will then bear evidence of normality or anomaly. High false positive rates are reported based on their simulation results.

Anomaly detection may be used to detect attacks against a network daemon or a SetUID program by building a normal profile of the system calls made during program execution. If the process execution deviates significantly from the established profile, an intrusion is assumed. Okazaki et al. [13] have proposed a lightweight approach using profiles consisting of the type of system call and its frequency occurrence, in which speech recognition methods is used to calculate the optimal match between a normal profile and a sample profile.

- Compared to the Misuse modeling, specification modeling takes the opposite approach; it looks for specification of how a system or program executes and marks a sequence of instructions as a potential intrusion if it violates the specification. This technique may provide the capability to detect previously unknown attacks, while exhibiting a low false positive rate.

4 Security architecture of the wireless part of the medical information system

Let us consider the medical information system infrastructure including the wireless sensor networks, as shown in Fig. 2. Due to the physical confinement of the healthcare central medical database should exist at the physically secure location. Medical record formed by data taken using wireless sensor network will be encrypted and timestamped and stored in central medical database. Other important parts of the architecture are the patient security processor (PSP) which is attached to bed and the wireless access point in the patient room. The PSP is module that implements networking as well as security-related functions.

From the application perspective, there are three application blocks which need to operate securely. They are: sensing with required event detection reliability, location reporting which accompanies sensed data and power management which determines sleep times for nodes in order to maximize the network life-time. They are inter-related because sleep time has to be determined according to the required event sensing reliability. All three services must have integrity, availability and potentially confidentiality. At the network layer secure routing has to be provided towards the medical database. Control packets for the routing algorithm be authenticated.

From the data link layer aspect, PSP is the cluster coordinator of sensing nodes which belong to the patient's body WSN and participates in the Medium Access Control function of the nodes. Sensing nodes will send packets with authenticated and potentially encrypted payload to the patient security processor which forwards them, possibly aggregated, to the room

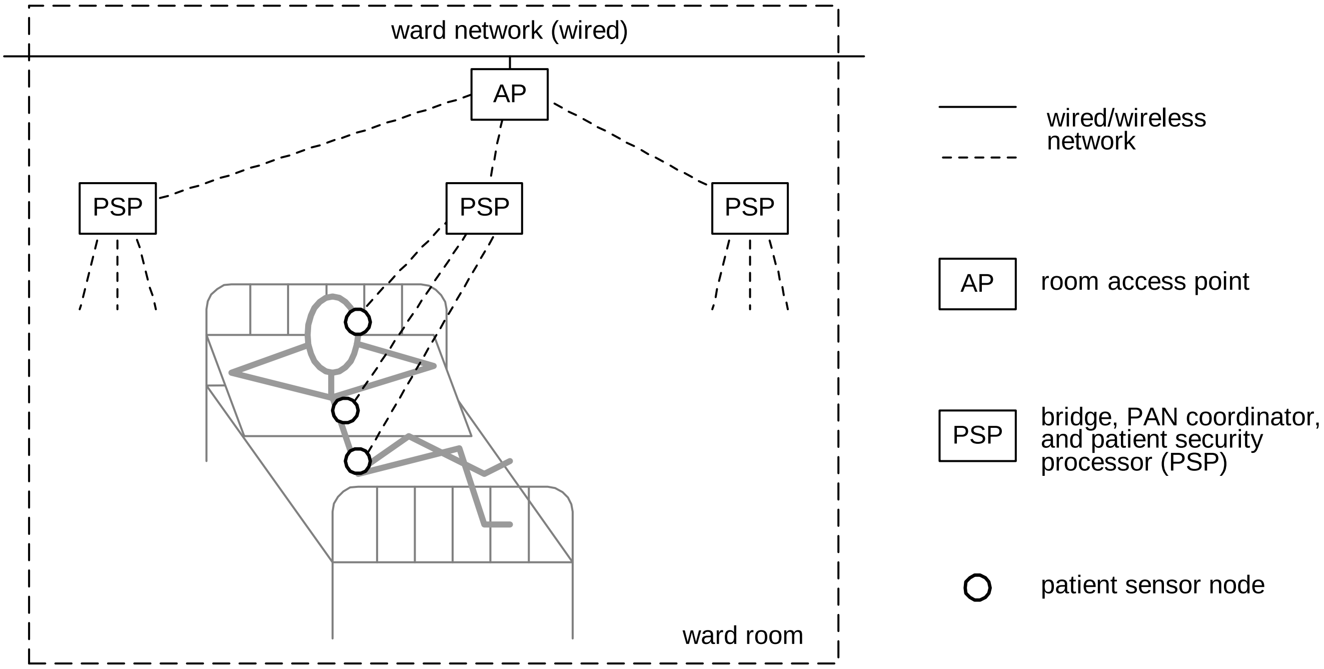


Figure 2. Security architecture of wireless part of medical information systems.

access point.

The patient's room access point is further connected to the central medical record database through a suitable wired network. The access point forwards encrypted and authenticated packets to the central database. From the networking point of view access point is interconnection device which interconnects Personal Area Network technology with the hospital network.

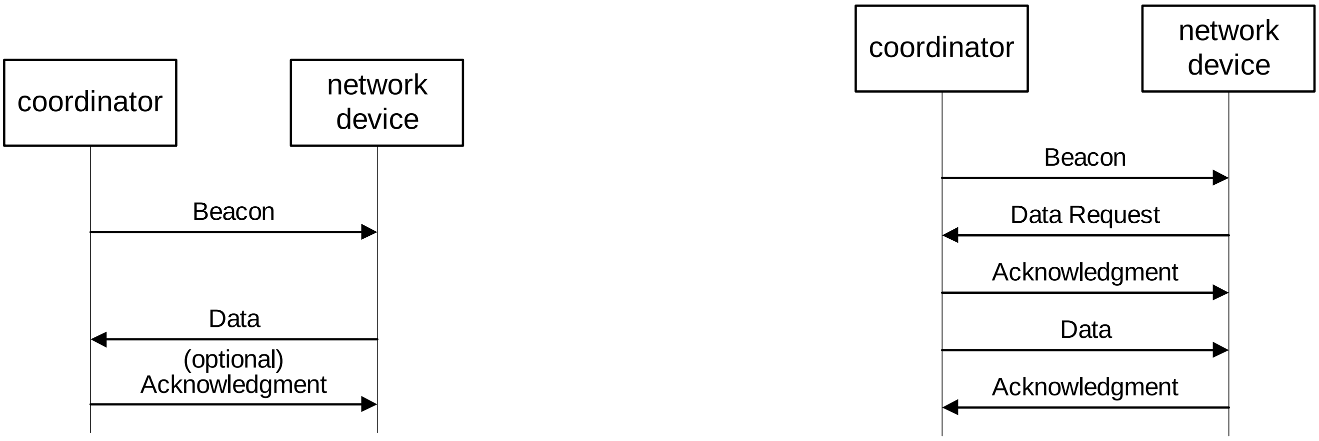
Medical personnel might carry their own PAN nodes and communicate directly to medical health database through the patient's room access point.

5 An overview of 802.15.4 specification

The 802.15.4 networks with star topology operate in beacon enabled mode where channel time is divided into superframes bounded by beacon transmissions from the PAN coordinator [4]. All communications in the cluster take place during the active portion of the superframe; the (optional) inactive portion may be used to switch to conserve power by switching devices to a low power mode. Standard supports 16 different frequency channels in which clusters can operate within ISM band.

Due to interference, physically adjacent clusters must operate in separate channels. Channel access is regulated through the slotted CSMA-CA mechanism [4].

Data transfers in the downlink direction, from the coordinator to a node, must first be announced by the coordinator. In this case, the beacon frame will contain the list of nodes that have pending downlink packets, as shown in Fig. 3(b). When the node learns there is a data packet to be received, it transmits a request. The coordinator acknowledges the successful reception of the request by transmitting an acknowledgement. After receiving the acknowledgement, the node listens for the actual data packet for the period of *aMaxFrameResponseTime*, during which the coordinator must send the data frame.



(a) Uplink transmission.

(b) Downlink transmission.

Figure 3. Data transfers in 802.15.4 PAN in beacon enabled mode.

The 802.15.4 standard specifies several security suites which consist of a ‘set of operations to perform on MAC frames that provide security services’ [4]. Specified security services include access control lists, data encryption using pre-stored key, message integrity code generated using the pre-stored key, and message freshness protection. While these services are useful, they are by no means sufficient. In particular, procedures for key management, device authentication, and freshness protection are not specified by the 802.15.4 standard. Hence, they must be implemented by the applications, or perhaps by another layer of network protocols running on top of 802.15.4 itself. Also, if the node hardware is not-tamper resistant, adversary can obtain keys, and access control lists from the node easily. It is possible to steal node’s identity and launch Sybil attack [12] and as a consequence read the patient’s health data (or transmit forged data). It is also possible to replicate node’s identity in foreign cluster which operates in the same frequency channel given that forged node is sufficiently close to the patient's body.

6 Symmetric-Key Key Establishment Protocol

Low cost alternative for this task with possibility to change the symmetric keys between the nodes and the coordinator is the ZigBee protocol suite [17] developed by the ZigBee Alliance, an industry consortium working on developing network and Application Programming Interfaces (API) for wireless ad hoc and sensor networks. The ZigBee APIs include security extensions at different networking layers, using both symmetric and asymmetric key exchange protocols. Asymmetric key exchange protocols, which mainly rely on public key cryptography, are computationally intensive and their application in wireless sensor networks is only possible with devices that are resource rich in computation and power and connected through high bandwidth links.

The application support sub-layer of the ZigBee specification defines the mechanism by which a ZigBee device may derive a shared secret key (Link Key) with another ZigBee device; this mechanism is known as the Symmetric-Key Key Establishment (SKKE) protocol. Key establishment involves coordinator and node, and should be prefaced by a trust provisioning step in which trust information (a Master key) provides a starting point for establishing a link key. The Master key may be pre-installed during manufacturing, may be installed by a trust center, or may be based on user-entered data (PIN, password).

This protocol relies on Keyed-hash message authentication code, or HMAC, which is a message authentication code (MAC) calculated using a cryptographic hash function in conjunction with a secret key. For the cryptographic hash function the 802.15.4 specification supports the AES block cipher in its basic form, while the ZigBee specification suggests the use of a modified AES algorithm with a block size of 128 bits [10]. The hash function of a data block d will be denoted as $H(d)$. The ZigBee specification suggests the use of the keyed-hash message authentication code (HMAC):

$$\begin{aligned} MacTag &= HMAC(MacData) \\ &= H((MacKey \oplus opad)||H(MacKey \oplus ipad)||MacData) \end{aligned}$$

where $ipad$ and $opad$ are hexadecimal constants. In this Chapter, we will follow the notation introduced in [17] and present the last equation in the equivalent form $MacTag = MAC_{MacKey}MacData$.

The SKKE protocol is initiated by the PAN coordinator (denoted as initiator device U) by exchanging ephemeral data. The PAN coordinator U will generate the challenge QEU. Upon receiving the challenge QEU, the node (denoted as V) will

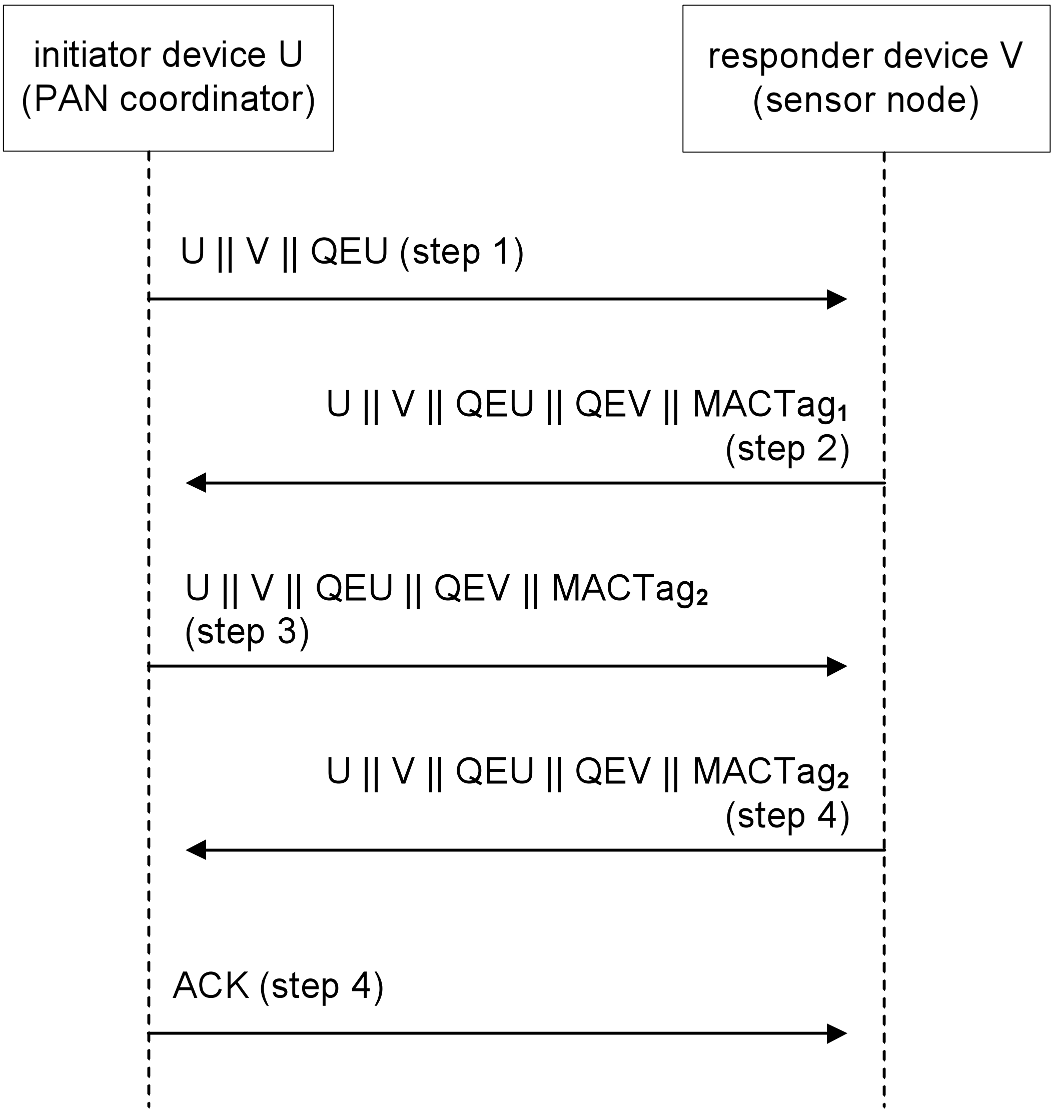

initiator device U (PAN coordinator)
responder device V (sensor node)
U || V || QEU (step 1)
U || V || QEU || QEV || MACTag₁ (step 2)
U || V || QEU || QEV || MACTag₂ (step 3)
U || V || QEU || QEV || MACTag₂ (step 4)
ACK (step 4)

Figure 4. SKKE protocol between the PAN coordinator and the node.

validate it and also generate its own, different challenge QEV and send it to the PAN coordinator U.

Upon successful validation of challenges, both devices generate a shared secret based on the following steps:

1. Each device generates a $MACData$ value by concatenating their respective identifiers and validated challenges together: $MACData = U||V||QEU||QEV$.

2. Each device calculates the $MACTag$ (i.e., the keyed hash) for $MACData$ using the Master Key $Mkey$ as $MACTag = MAC_{Mkey}MACData$. Note that both devices should obtain the same shared secret $Z = MACTag$ at this time.

3. In order to derive the link key each device generates two cryptographic hashes of the shared secret and hexadecimal

numbers, i.e. $Hash_1 = H(Z||01_{16})$ $Hash_2 = H(Z||02_{16})$. The $Hash_2$, will be Link Key among two devices, while $Hash_1$, will be used to confirm that both parties have reached the same Link Key.

7 Analysis of possible attacks

From the point of view of general sensor network, following attacks have been described in the literature:

sybil attack - malicious node takes fabricated identity or it presents multiple fabricated identities in the network [12].

sinkhole attack - malicious node tries to get all the traffic from particular area which can potentially result in the DoS attack.

blackhole and grayhole attack - malicious node drops all or some traffic received from the other nodes.

wormhole attack - malicious node captures packets from one part of the network and forwards them through dedicated channel to another malicious node. It can target routing function or application when it is usually coupled with the sinkhole attack [6].

sleep attack - node sleeps less than is needed than it can bias the results and it will exhaust its battery before the others [14]. If it sleeps more than needed, event sensing reliability is not accurate .

fairness attack - node sends more packets to the coordinator (even without the sleep policy) then the other nodes it can bias the sensing results.

denial of service DoS attack - usually performed at the MAC layer in order to exhaust node's battery by permanent packet re-transmissions.

However, there is a large amount of cross-layer interaction in protocol layers of sensor network. For example, power management naturally belongs to the application layer which knows the required event sensing reliability in the cluster. However, power consumption for nodes in the cluster depends on the routing decisions and amount of packet collisions. Therefore, all three layers must cooperate in order to determine the sleep period per node which will result in required event sensing reliability. Also, integrity of sensing, location and power management function can be provided by Message Authentication Code using the symmetric key calculated in Section 6. If different keys are needed for each application part (i.e. sensing, location and power management) SKKE algorithm can be extended to provide independent key for each application function. Therefore, we consider attacks which affect the key distribution process either for particular node or for the whole cluster. Since key distribution algorithm is implemented on top of the MAC layer we exploit joint vulnerabilities of the SKKE and cluster based 802.15.4 MAC.

Under the architecture of the medical wireless sensor network using the star based 802.15.4 technology the attacks take special form. We will also classify the security attacks as attacks on node and attacks on PAN coordinator (or Patient Security Processor) and relate them to general attacks. We note that even with link key updates, Sybil attacks [12] and further attacks which result from their success are still possible.

Attacks on nodes Nodes are in close vicinity of patient's body and we feel that it is reasonable to have only few nodes under the attack. Since node's hardware is not tamper-proof it is possible to read the ID and master secret from its ROM, and wait for the time when PSP initiates new Link Key update in order to compute the new Link key. Node MAC addresses which are actually node identities can be 16 bits or 64 bits long. If 16 bit node IDs are chosen in order to save the space in packet header, node ID might even be fabricated in the time range which can make this form of sybil attack feasible.

Even with small number of corrupted nodes it is possible to attack the fair bandwidth allocation in the body WSN due to CSMA-CA type of access. Malicious node(s) can try to access the medium more frequently than the other nodes which will increase the access delay and packet loss for good nodes. This attack can be prevented if PSP keeps the track about the number of packets received from each node during some time period.

Corrupted node can also attack the key distribution process since the coordinator (PSP) announces the IDs of nodes who are about to change the link key in plain-text in the beacon frame. Therefore, attacker can send request packet with the ID of the legitimate node. As the result, PSP will start the key-exchange process when the recipient node is not ready and it will be stuck in the algorithm handshake. This attack can be prevented if request packets are authenticated with the MAC code and if PSP has time-outs in its key exchange process. The more brutal outcome of this attack is a simple collision of request packets which prevents good node from completing the key update process. This can be classified as DoS on the key exchange.

Situation gets more difficult if node applies some power saving technique and sleeps for random periods of time [11]. Such techniques are applied in order to extend the lifetime of the network while achieving required event sensing reliability. Randomizing the sleep time spreads nodes activities uniformly over the time. In that case attacker can just appear as a legitimate node which has waken up while the real node is sleeping (assuming that attacker has secret key) or is captured and destroyed. In order to deal with this attack, PSP has to keep the average of the sleep periods and isolate the node which wakes up more often than the others.

Attacks on coordinator (PSP) Attacks on PSP (coordinator) can be much more harmful than the attacks on ordinary nodes since PSP is forwarding all measurements to the central information system.

1. Adversary may read the contents of beacon frame as well as contents of all data frames if they are not encrypted. Finding the frequency channel of particular body network is not difficult since there are only 16 of them. From the sequence of beacon frames, adversary may learn node IDs. It can also hear requested event sensing reliability and number of nodes and from these numbers it can calculate parameter of the sleep time probability distribution [11].

2. From the beacon, attacker can also learn the period of key exchange since coordinator advertises the MAC address of the node which security packet counter has reached the threshold value. One way for dealing with this problem is to encrypt the data in the beacon with the group key which will prevent passive listening.

3. Location of the PSP has to be securely reported to the central database. Location of the PSP can be determined with the collaboration of surrounding PSPs which have GPS receivers or by using node's own GPS. The first approach is similar to the location discovery algorithms [8] where PSP does not have GPS but it can hear beacon frames from other PSPs with GPSs and determine its relative location with respect to its neighbors based on the power of the received signal. This approach can be attacked with the adversary which has higher powered transmitter. As the result, PSP will report measurements from the wrong location which will not be accepted by the central database. This attack can be combined with substituting the forged PSP with correct location. Recent work [9, 7] attempts to detect malicious nodes in location detection algorithms, but there is an issue how harmful this attack can be while it is not detected. If PSP has its own GPS but it does not participate in localization algorithms it is possible that adversary gets in the reach of the whole PSP and forges location and data. In our opinion, PSP should have its own GPS but it should also participate in location detection algorithm with its neighbors.

4. It is possible that two corrupted distant PSPs establish a channel (due to the issue of physical security we assume that this will be wireless channel also). Then, one PSP can forward the data to the other which can report them as measurements. This is similar to a wormhole attack which was first introduced as the attack on the routing algorithms

[3, 5] followed by the grayhole/blackhole/sinkhole attack. Since no other PSPs are affected it is very difficult to detect this attack using collaborative algorithms among PSPs. Instead, it is necessary to check the activities on the wireless channels which are not in use by the neighboring PSPs.

5. If the PSP's hardware is not tamper free, then it can be temporarily stolen and master secrets for the nodes can be read. However, for the applications which require high level of confidentiality of medical data, we hope that PSP's hardware will be tamper-free or/and it will be kept at secure location.

8 Conclusion and Future Work

We have discussed potential security attacks on healthcare network implemented over IEEE 802.15.4 beacon enabled clusters. We note that physical security of PSPs is crucial for the secure network operation. In our future work we will implement intrusion detection system for healthcare network based on misbehaving signatures of the attacks listed in this work.

References

[1] M. Bishop. *Computer Security – Art and Science*. Pearson Education, Inc., Boston, MA 02116, 1st edition, 2003.

[2] A. F., D. Subhadrabandhu, and S. Sarkar. Signature based intrusion detetcion for wireless ad hoc networks. In *Proc. Vehicular Technology Conference, Wireless Security Symposium*, pages 1069–1082, 2005.

[3] Y.-C. Hu, A. Perrig, and D. Johnson. Ariadne: A secure on-demand routing protocol for ad hoc networks. In *Proc. ACM Mobicom 2002*, pages 12–23, 2002.

[4] Standard for part 15.4: Wireless MAC and PHY specifications for low rate WPAN. IEEE Std 802.15.4, IEEE, New York, NY, Oct. 2003.

[5] C. Karlof and D. Wagner. Secure routing in sensor networks. In *Proc. 1st IEEE International Workshop on Sensor Network Protocols and Applications 2003*.

[6] I. Khalil, S. Bagchi, and N. B. Shroff. Liteworp: a lightweight countermeasure for the wormhole attack in multihop wireless networks. In *Proc. 1st IEEE International Conference on Dependable Systems and Networks DSN 2003*, pages 612–621, 2005.

[7] L. Lazos and R. Poovendran. Serloc: Robust loacalization for wireless sensor networks. *ACM Transacations on Sensor Networks*, 1(1):73–100, 2005.

[8] J. Li, J. Jannotti, D. De Couto, D. Karger, and R. Morris. A scalable location service for geographic ad hoc routing. In *Proc. ACM Mobicom 2000*, pages 120–130, 2000.

[9] D. Liu, N. P., and W. Du. Detecting malicious beacon nodes for secure loaction discovery in wireless sensor networks. In *Proc. International Conference on Distributed Computer Systems, ICDCS 2005*, pages 609–619, 2005.

[10] A. Menezes, P. van Oorschot, and S. Vanstone. *Handbook of Applied Cryptography*. CRC Press, 1997.

[11] J. Mišić, S. Shafi, and V. B. Mišić. Cross-layer activity management in a 802.15.4 sensor network. *IEEE Communications Magazine*, 44(1):131–136, Jan. 2006.

[12] J. Newsome, E. Shi, D. Song, and A. Perrig. The Sybil attack in sensor networks: Analysis and defenses. In *Proceedings of IEEE International Conference on Information Processing in Sensor Networks (IPSN 2004)*, pages 259–268, Berkeley, CA, Apr. 2004.

[13] Y. Okazaki, I. Sato, and S. Goto. A new intrusion detection method based on process profiling. In *Proc. Saint: Symposium on Applications and the Internet*, pages 82–91, 2002.

[14] M. Pirretti, S. Zhu, Vijaykhrishnan, McDoniel, and M. Kandmir. The sleep deprivation attack in sensor networks: Analysis and methods of defense. *International Journal of Distributed Sensor Networks*, 2:267–287, 2006.

[15] D. Subhadrabandhu, S. Sarkar, and A. F. Rida: Robust intrusion detetcion in ad hoc network. In *Proc. 4th International IFIP-TC06 Networking Conference*, pages 1069–1082, 2005.

[16] Y. Zhang and W. Lee. Intrusion detetcion in wireless ad hoc networks. In *Proc. 6th International Annual Conference on Mobile computing and networking, MobiCom'00*, pages 275–283, 2000.

[17] ZigBee specification. ZigBee Document 053474r06, ZigBee Alliance, San Ramon,CA, 2005.