Security for Pervasive Health Monitoring Sensor Applications

Krishna K. Venkatasubramanian, Sandeep K. S. Gupta
Department of Computer Science and Engineering, Arizona State University
Tempe, Arizona, 85287, USA,
{*kkv,sandeep.gupta*}*@asu.edu*

Abstract

Maintaining security of wearable networked health monitoring sensors (Body Sensor Networks (BSN)) is very important for the acceptance and long term viability of the technology. Sensors in BSNs organize themselves into different topologies for efficiency purpose. Securing these topology formation process is of prime importance. In this paper we present two schemes which rely on the novel technique of using physiological values from the wearer's body for securing a cluster *topology formation. Traditional schemes for cluster (one of the most commonly used topology) formation were not designed with security in mind and are susceptible to security flaws. The schemes proposed here not only solve the secure cluster formation problem but also do so efficiently by eliminating all key distribution overheads. We analyzed the security of the protocols and tested their accuracy on a prototype implementation developed using Mica2 motes.*

1. Introduction

Recent developments in miniaturization and low-powered electronics has lead to the development of wearable health-monitoring systems which provide us with the capability of automated, continuous patient monitoring. These systems are usually equipped with a large number of tiny, non-invasive sensors, located on or close to the patient's body, for health monitoring purposes. Such systems are being designed to measure diverse physiological values including Blood Pressure (BP), Electrocardiogram (EKG), Blood Oxygen level (Sp02), activity recognition etc. and are available in many different forms including - wrist wearable, ambulatory devices and as part of biomedical smart clothes [1] [2]. We call these wearable health monitoring systems as Body Sensor Networks (BSN) and define them as - a network of wearable heterogeneous sensors, spread over the entire body, having the ability to measure and communicate a myriad of health related stimuli.

The Health Insurance Portability and Accountability Act (HIPAA) [3] mandates that, as the sensors in BSN collect the wearer's health data (which is regarded as personal information), care needs to be taken to protect it from unauthorized access and tampering. In all sensor networks, sensors sense their environment and forward the data obtained to a controller entity called Base Station (BS), either directly or through other sensors in the network. Protocols for inter-sensor communication have traditionally relied on the presence of a secure key distribution and management infrastructure for maintaining confidentiality and integrity of the information transmitted. In this paper we improve this process by proposing a novel scheme which uses the physiological values, from the wearer's body, directly as cryptographic keys. Such a scheme is helpful in decreasing the complexity of the overall security protocol, and also improve its efficiency by reducing its communication complexity, as it eliminate the requirement of key distribution.

In our preliminary work [4], we developed a protocol for performing the basic secure inter-sensor communication using physiological values from the wearer's body. In this paper we expand the idea and use it for securing topology formation in BSN. As mentioned before, sensors, on sensing their environment, send their data to the BS, for further processing. Sending data directly to the BS can be expensive as sensors are highly constrained in communication capabilities [5]. It has been shown that organizing sensors in efficient topologies, like clusters, can help reduce communication costs [5]. Clusters are a group of co-located sensors which delegate one sensor (for short durations) among them to perform direct communication with the BS. Traditional cluster formation protocols depend on signal strength information of the control messages for forming clusters. This technique has serious security flaws which can potentially allow malicious entities to take over the entire network [6]. Our *contributions* in this paper are two secure cluster formation protocols which mitigate the aforementioned security flaws by using physiological values (PV)[1], from wearer's body, for providing the required security. The use of PVs eliminates the cost of key distribution and management, further prolonging the BSN's life and usability.

The rest of the paper is organized as follows: Section 2, presents the motivation of the problem. Section 3, 4 5 an 6 present the system model, problem statement, keying structure used and physiological value based security, respectively. Section 7 presents the two protocols, followed by security analysis and prototype implementation in Section 8 and 9, respectively. Section 10 presents the related work and Section 11 concludes the paper.

2. Motivation

Clusters are useful in BSN, because they allow for large energy savings due to reduced communication and data fusion at the leader nodes. As an example, consider a BSN with large number of Activity Recognition Sensors (ARS) spread

[1]Physiological parameters can be used to securing any type of communication within a BSN, including techniques for organizing sensors in different topologies, In this paper, we focus on demonstrating the use of PVs for securing cluster topology formation.

throughout the wearer's body. ARS sensors are used for determining the activity performed by the wearer such as sitting, walking, running etc and is normally used in tandem with other health monitoring sensors to provide a better information on the current condition of the wearer. For example: if the wearer's BP is very high after a jog, the results can be interpreted accordingly. ARS therefore provides the correct context for interpreting health data collected from a wearer. As most human activities are characterized by specific motions of distinct body parts (walking involves the movement of our arms and legs in a systematic manner), any such movement can be detected by all the ARS in that area and reported to the BS. Forming clusters among sensors can improve system reliability and reduce the amount of data (by data fusion at the leader) being sent in such situations compared to the scenario where each sensor in the wearer's leg sends its data directly to the BS for each leg movement observed.

So far, a large portion of BSN research has been carried out with a few high precision sensors located at specific part of the patient's body. Though accurate, such systems are bulky (potentially limiting patient's movements), have high energy needs and are not conducive to long-term monitoring. In [7] it has been shown that deploying large number of tiny, poor quality sensors in place of a few good ones can be very useful because they do not seriously harm the quality of the measured data, they do not interfere with the patient's daily routine, and they have lesser energy requirements. We therefore contend that for usability reasons BSNs will consist of a dense network of sensors in which specific topological organizations will be useful in improving their efficiency.

3. Problem Statement

In this section we will describe the problem associated with cluster formation process. In any clustering scheme the nodes are divided into different virtual groups based on pre-existing rules. Each cluster has a designated Leader Node (LN), which coordinates the activities of the other nodes in the cluster by performing data forwarding and data fusion. There is only one LN per cluster. In the rest of the paper we refer to the leader node as LN or leader and the non-leader nodes as Other Nodes (ON). We consider single level clusters in this paper, forming multi-level hierarchical clusters are a simple extension.

Traditionally, clusters are formed, in a distributed manner, around a set of elected LNs. If we assume W to be the set of all sensors in a network, and M and N to be the set of elected LNs and the set of ONs in the network respectively (i.e. $|N| = |W| - |M|$), then the cluster formation process takes place in the following three steps: **Step 1: Broadcast Solicitation:** Each LN $p \in M$ broadcasts a solicitation beacon which contains its id and other control information. There are a maximum of $|M|$ solicitation beacons broadcasted in this step. The presence of a communication schedule is assumed along with the synchronization of the sensor clock using schemes such as in [8]. **Step 2: Leader Node Selection:** Each of the $|M|$ solicitation beacons is received by a subset of the total number of sensor nodes in the network. Each sensor $q \in N$, which has received at least one solicitation, then chooses as its LN a node $j \in M$, such that, out of all the beacons received by q, $s_j = max(s_1, s_2, ..s_h)$, where s_k is the signal strength of the solicitation beacon from LN k and $h \leq |M|$. **Step 3: Transmitting Reply:** Each sensor $q \in N$, transmits a reply message to the chosen LN, thereby joining its cluster.

An inherent problem with this protocol is that: in Step 1, the ONs assume that only the elected LNs broadcast the solicitation beacon and that each elected LN is trustworthy. Therefore when they chooses a LN in Step 2, they do not know if they are joining a cluster of a legitimate LN or a malicious entity posing as legitimate LN.

The presence of the aforementioned problem can lead a malicious entity to broadcast a much stronger solicitation signal (than all legitimate LNs) in Step 1 and fool the sensor nodes into making it as their LN. In [6] this attack is referred to as *HELLO Flood attack* and the malicious entity thus forms what are called *sinkholes* for all the sensors which designated it their LN. Once a sinkhole is formed, it can control the communication of the sensors that forward data to it, leading to attacks like, data integrity loss, and selective forwarding of data [6]. The problem cited in [6] was presented with traditional sensors in mind and not BSNs, but the same applies here given the fact that BSN can potentially contain large number of sensors and sensors in a region react to an event at the same time. Similarly, a LN also assumes that the reply it received in Step 3, was from a completely trustworthy ON thereby allowing a malicious entity to join a cluster and potentially generate bogus information.

Finally, it needs to be clarified that we focus only on securing the cluster formation process and do not address the leader selection process as many of the previous works in this domain have attempted [9][10][11][12][5]. We assume here that leader selection has already been done using any of these schemes and we focus exclusively on what happens thereafter.

4. System Model

This paper presents secure cluster topology formation protocol for a BSN. The BSN consists of a dense network of low quality wearable physiological and activity monitoring sensors which are distributed all over the wearer's body. All these sensors report to, and are controlled by a Base Station (BS). The sensors are built to survive extreme conditions like variation in temperature and presence of water [13]. All sensors communicate using the wireless interface and do so reliably using schemes such as those presented in[14].

The BS is the controlling entity of this architecture. There is only one BS controlling the entire BSN and all the sensors in the BSN are within its reach. The BS is the gateway of the BSN to the outside world and is assumed to have sufficient computational and communication capabilities. The sensor nodes in the BSN are heterogeneous. Further as the sensors need to operate continuously for long periods of time, we assume the presence of powering mechanisms like using body movements, body heat production, flexible solar cells etc [1].

The following are the trust and threat assumptions for our system: 1) The wireless medium, which is broadcast in nature, is not trusted. All messages received have to be authenticated before being accepted; 2) The BS is completely trustworthy and can never be tampered with; 3) We consider the BSN to be deployed on an ambulatory patient and therefore rule out physical sensor compromise; 4) We do not address physical layer security issues in this work like signal jamming; 5) The

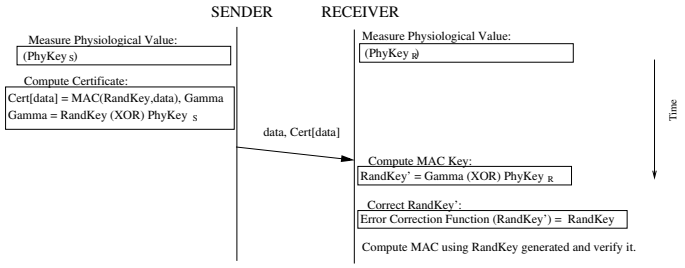


Fig. 1: Using PVs for Authenticated Inter-Sensor Communication

cryptographic primitives used are assumed to be error free and vulnerabilities from social engineering are not addressed. Before we go into the details of our protocols we present some preliminaries about the cryptographic keys used and the use of PVs in securing communication in the next two sections.

5. KEYING STRUCTURE

We use symmetric key cryptography in our design, mainly because the use of Public Key Infrastructure (PKI) is expensive for long-term usage in a BSN [15]. The keying structure employed is as follows - each node in the system shares a pre-deployed pair-wise master key Km with the BS. Even though we assume node compromise is not possible, we refrain from using a system wide shared key mainly because- 1) the range of values transmitted by the sensors is limited and 2) the amount of data generated is potentially large. The adversary listening to the communication can therefore easily mount cryptanalytic attacks on the system and obtain this shared key which could compromise the whole network. Further, we do not use Km directly in communication but generate two *derived* keys from it and use them instead. This prevents the loss of the master key even if the communication security is compromised by any cryptanalytic attack. The two derived keys are defined as- $K'_{X-BS} = H(Km, 1)$, $K'_{BS-X} = H(Km, 2)$, where the first key is for all messages sent from the sensor to the BS while the latter is for BS to sensor communication and H is a cryptographically secure one-way hash function, which takes two parameters - the master key and an arbitrary number to generate the required derived key. We now present the PV based security scheme which uses this keying structure.

6. PHYSIOLOGICAL VALUES BASED SECURITY

Securing (term is used in a generic sense and should be read so as to mean any or all of the following: encryption, authentication, and integrity maintenance) any communication between two entities requires the distribution of a shared secret (not considering public key based schemes) between them which can be used as a tool to hide the exchanged information. Distributing a shared secret (usually a cryptographic key) between the communicating entities securely is a challenge and numerous protocols have been published over the years to efficiently solve the problem [16] [17]. We however take a slightly different view here. We contend that as sensors are usually placed in remote environments, they could use the specific properties of these environments itself for generating shared secrets, though not all environments are conducive for this purpose. The environment has to be dynamic, and its properties random enough to prevent any brute-force attacks on them. The human body is one such environment. In this context of BSN, the sensors could use Physiological Values (PV) from the body (for example: Heart Rate, and Blood Glucose Level) for this purpose. Not all PVs are however suitable for being used for cryptographic purposes. An ideal PV would be the one which is universally (in the body) measurable, unique, time-variant and is random enough to prevent guessing.

In [18], the authors have proposed the use of Inter-Pulse-Interval (IPI) for securing inter-sensor communication in a biosensor based network. Heart Rate Variance (HRV) is another PV which has been shown to be ideal for securing inter-sensor communication [19]. In both cases it has been shown that these PVs are unique for each individual. Measurement of the same PVs on two different individuals produces substantial variations with Hamming distances of up to 80 bits [19]. It needs to be noted however, that we cannot choose a couple of PVs for a whole network and expect all sensors to be able to measure it. In real systems we contend that, when two sensors want to communicate, they will first exchange a list of PVs [2] that they can measure and then choose one they both support, much like the protocols like SSL which have provisions for choosing encryption algorithms. Interesting work relating to the usage of EKG [21] and Photoplethysmogram (PPG)[22] have been proposed to uniquely identify individuals, any of these schemes can be easily ported here. Discovering additional PVs which are suitable for cryptographic purposes is crucial for acceptance of this technique and an open research problem.

Figure 1 shows protocol for using PVs in securing communication between two sensors in the BSN (using them for encryption is a trivial extension). Here, the sender generates a *physiological certificate* using a chosen PV. The certificate is defined as $Cert[data] = MAC(RandKey, Data), \gamma$ where $\gamma = PhyKey_s \oplus RandKey$ ($\oplus$ represents the XOR operation). The values $RandKey$ is just a random number used as a key to compute the Message Authentication Code (MAC) on the $data$, while $PhyKey_s$ is the PV measured at the sender. The γ is used to send the $RandKey$ value across to the receiver (for enabling MAC verification) by hiding it using a one-time-pad generated over $PhyKey_s$. The receiver too measures the PV at its end $PhyKey_r$ (at the same time as the sender), which it uses to compute the $RandKey' = \gamma \oplus PhyKey_r$, for verifying the MAC.

The human body has a dynamic nature, and shows topographic specificity. Therefore, a specific PV measured at one part of wearer's arm, will be different from any value measured at the leg or torso for instance. However, the PVs measured at two points on the arm will be very close [23]. As the sensors in the BSN are small, densely deployed, and have small communication ranges, we contend that sensors will be able to communicate with only those which are close to its location and therefore the PVs measured at the two communicating sensors will vary only slightly. Therefore the value of $RandKey'$ obtained at the receiver may not be equal to the one generated at the sender $RandKey$. [24], [4] observe that the measurements at sender and receiver are independent of each other and one can use simple error correction scheme

[2] Already physiological monitoring sensors are becoming multi-modal and are being able to sense multiple types of stimuli [7][20]

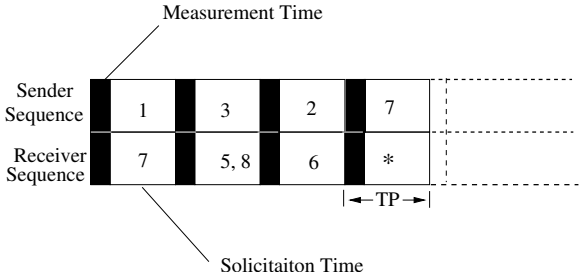


Fig. 2: Sample PV Measurement and Transmission Schedule

to correct the situation. We assume that such a scheme is applied here (i.e. $RandKey = f(RandKey')$, where f is an error correction function) to resolve the difference in $RandKey$. The resulting value is then used to verify the MAC, thus verifying the sender. One of the important properties of the PV chosen for securing inter-sensor communication is that they are time-variant and vary unpredictably. This prevents malicious entities from guessing the PVs. For this reason any PV measurement, at both sender and receiver, has to be done at the same time. In Figure 2, we present a sample schedule which the senders and receivers must follow to be able to successfully use PVs for inter-sensor authenticated communication. Further, at this point we also assume that the sensors which are going to communicate have already decided on a common PV they are going to use. Such a schedule could be decided by the BS, depending upon the communication needs and broadcasted to all the sensors in the network.

The communication schedule, is divided into time-periods (TPs). Each TP consists of a sender and at least one receiver. In Figure 2, sensors 3 is the sender and sensors 5 and 8 are the receivers for TP2, in TP4, node 7 is the sender and everyone else is the receiver and so on. Both the sender and receiver(s) measure the [agreed upon] PV at the the Measurement Time (MT) of the time-period they are assigned to. The senders then transmit their data along with the certificate in their alloted Solicitation Time (ST) within their time-periods to the receiver(s), which, use their version of the PV to verify the certificate and authenticate the data. In the next time-period the same procedure continues for different (or possibly same) pair of sender and receiver(s). Each time two nodes have to communicate, they measure the PVs afresh, old PVs are never reused. The presence of time-periods prevents interference and ensures that even if, in two TPs, the same PV is used for generating physiological certificates, the actual values used are different and not predictable.

7. Secure Cluster Formation Protocols

The main reason traditional cluster formation protocols suffer from HELLO Flood Attack and sinkhole formation is because of the lack of authentication in the inter-sensor communication. Therefore any arbitrary entity can pose as a leader and send cluster forming solicitation messages. Here we present two protocols which alleviate this problem.

Centralized Protocol In both of our protocols we assume that the LNs have been chosen based on some mechanism such as [5]. The idea behind this approach is to ask the BS to form clusters within the network rather than allowing the decision to be made by individual sensor nodes as is traditionally done. Figure 3 shows the protocol's three steps. In the first step, the ONs broadcast a *solicitation* in order to join a cluster along with their physiological certificate (S1,S2,S3). We assume that a suitable schedule is present for this. The LNs which receive this solicitation, verify the certificate and *relay* the message to the BS along with information on the signal strength (SS), at which they received the solicitation, appended to it (R1-R5). Finally, the BS, which receives many copies of a ONs' solicitation from different LNs, chooses the LN whose SS value was the highest, and sends a *reply* back to each ON in the network.

Each step of the protocol requires proper authentication. The ONs have to include the physiological certificate in their solicitations to prove that they are genuine to the LNs. Their solicitations themselves are composed of a MAC, computed over the key (K'_{X-BS}) they share with the BS, for authenticating themselves to the BS. The LNs which forward the solicitations also have to authenticate themselves to the BS using a shared key. The BS can thus prevent any LN from becoming the cluster leader if it is not satisfied with the authentication result, thus preventing a malicious entity from becoming the cluster leader. Similarly, if the BS is not satisfied with the MAC in the solicitation messages (sent by the ONs) it is discarded. The protocol is secure (in terms of cluster leader selection) even if the PV is compromised, albeit, at the cost of LNs potentially forwarding bogus messages sent to it by a malicious entity. We discuss this issue in the next section.

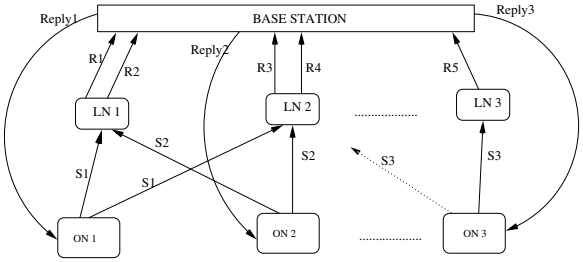
Distributed Protocol This protocol extends the traditional cluster formation scheme by including a physiological certificate with the solicitation sent by the LNs. The reply from the ON (which choose their LN is based on the received signal strength) to their LN also contains a physiological certificate to verify their identity as being from the same BSN network. Figure 4 shows the protocol steps. It can be seen that the distributed protocol is much more efficient than the centralized one because it does not involve the BS, however its security relies solely on the strength of the PV.

8. Security Analysis

In this section we present a brief analysis of the security provided by our protocols. **Possible Vulnerability** An adversary can spoof the identity of a legitimate LN and mount a HELLO Flood attack by broadcasting a extremely strong solicitation beacon, in an attempt to form sinkholes, or relay ON solicitations with large SS values to the BS to attract more ONs in its cluster [6].

Prevention In the centralized scheme, this attack is not possible because when the LNs relay the solicitation beacon from a non-leader sensor node to the BS, they have to include a MAC computed using the key (K'_{X-BS}) they share with the BS to authenticate themselves. An adversary does not have the necessary derived key and therefore cannot authenticate itself. For the distributed scheme, the physiological certificate is used to authenticate LNs and the rest of the sensors. As an adversary is not in contact with the body (and we assume any such contact can be noticed by the wearer and therefore will not be attempted) it cannot measure the PV and hence cannot create the certificate.

Possible Vulnerability An adversary can spoof the identity of a sensor node or a BS and try to become a part of the network or send bogus information or solicitations.



Solicitation: $N_k, Nonce_k, MAC(K'_{N_k-BS}, Nonce_k)$, $Cert[N_k, Nonce_k]$
Relay : $N_k, Nonce_k, MAC(K'_{N_k-BS}, Nonce_k), N_p, SS$, $MAC(K'_{N_p-BS}, N_p|SS)$
Reply : $N_z, MAC(K'_{BS-N_k}, N_z|Nonce_k)$

Here: k, p and z are the index of all soliciting ONs, LNs and those LNs which are chosen as leaders respectively
$Nonce_x$ is nonce generated by node 'x' for maintaining transaction freshness

Fig. 3: Centralized Cluster Formation Protocol

Prevention In the centralized scheme an adversary posing as a sensor node (ON or LN) needs to generate a MAC for the BS and a physiological certificate for the LN to verify. As it is not part of the network, it does not share a key with the BS nor can measure any PV and therefore will not be able to pose as a sensor node. For the distributed scheme as the adversary does not have the necessary PV, it cannot generate or verify the certificate. Similarly, for either case, an adversary cannot pose as a BS because it would have to append a legitimate MAC to any message it communicates, using the key K'_{BS-X}, which it cannot do.

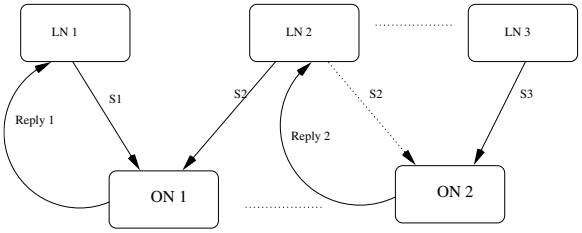
Possible Vulnerability If a malicious entity is able to break the physiological value based certificate and spoof PV, the HELLO-Flood attacks resulting in sinkholes is possible.

Prevention In the centralized scheme the compromise of PV would still not compromise the cluster formation process. Albeit, now it would be easier for malicious entities to send bogus solicitations, to the LNs, to be forwarded to the BS. However, as they cannot include MAC, for the BS to verify, their solicitations will be disregarded. The only downside for this scheme is that DoS attacks are possible on the LNs, as they can be duped into forwarding large number of bogus solicitation messages to the BS. This is a problem we are trying to address as of now. The distributed scheme will fail completely if the PV is ever compromised. The choice of PVs for cryptographic purposes is therefore very important to prevent such problems.

9. Prototype Implementation

We have prototyped both the centralized and distributed protocol on an actual network of sensors. The aim of this prototype development was to test the implementability and security of both the protocols and provide a proof of concept. The sensor network was built using UC Berkeley MICA2 motes and were programmed using the TinyOS environment. Each mote had a 8MHz ATMega128L micro-controller with 128KBytes of programmable flash and 4KBytes of RAM. The motes are powered by 2 AA batteries (http://www.xbow.com).

The prototype was implemented using a network of sensors consisting of 1 BS, 3 LNs and 4 ONs with a couple of adversaries attacking it during the cluster formation process



Solicitation: $N_p, Nonce_p, Cert[N_p, Nonce_p]$

Reply: $N_s, N_d, Cert[Nonce_d, N_d, N_s]$

Here: s, d and p are index of ONs, chosen LNs and broadcasting LNs, respectively
$Nonce_x$ is a nonce included by node 'x' for maintaining transaction freshness

Fig. 4: Distributed Cluster Formation Protocol

(no BS was used for the implementation of the distributed protocol). We monitored the communication taking place in the two protocols using a special *listener* node which was programmed to listen in promiscuous mode. The listener node sent its data to a connected PC which displayed them.

For the centralized protocol, we used three types of messages: 1) *SolicitMsg* which contained the initial solicitation sent out by the sensor nodes, 2) *RelayMsg* which is the solicitation relayed by the LN to the BS with added parameters like signal strength, 3) *ReplyMsg* which is sent by the BS to the sensors (other than LNs) containing the id of their leader. In the distributed case we just used the *SolicitMsg* sent by the LNs and *ReplyMsg* sent by the sensor nodes to their chosen leaders. We used CBC-MAC generated the Message Authentication Code at each step. An important requirement of our protocols was the measurement of PVs. We did not perform actual measurement on the fly for the chosen PV but assumed their values. The size of the binary files that was uploaded to the motes was 15.2KB for the BS, 12.5KB for the LN and 13.5KB for the ONs in the centralized protocol. For the distributed case the LNs and ONs binary files were 12.8KB and 13.9KB respectively. It can be seen that the protocol implementations are extremely lightweight in terms of code size. To test our development, we simulated some attacks on it. In the first case, we programmed one of the adversary mote to spoof the identity of a LN to try to become a sinkhole of the network. For the centralized protocol the adversary mote reported extremely high signal strengths while forwarding the solicitations received by itself, from the ONs, to the BS. But this did not lead to sinkholes because, the MAC appended by the adversary (to authenticate the signal strength) failed to match. Consequently the BS discarded the solicitations received from the mote posing as the adversary. For the distributed protocol, the adversary did not have appropriate PVs and therefore the ONs did not accept its solicitation (certificate did not match) thus preventing the HELLO-Flood attack and consequently sinkholes.

In the second case we made the adversary mote pose as a legitimate sensor node, which then tried to infiltrate the network. For the centralized protocol, the solicitation sent out by our malicious sensor node was dropped by the BS as the MAC did not match. In the distributed case, the malicious sensor node could not send a valid reply to the solicitation sent by a LN due to lack of knowledge of appropriate PV. We tried

simultaneously attacking our network with two adversaries; one posing as a LN and the other as sensor node. Both the adversaries were left out of the network after the clusters where formed, in both protocols for reasons given above. The results from the prototype development were thus in order with the security analysis presented previously.

10. Related Work

Little attention has been given to security in health monitoring till now. Most of these protocols developed so far require costly key distribution process [25] to be able to ensure secure communication. Using the human body directly for this key generation and distribution has a big advantage in this regard. One of the first works which utilized PVs for securing inter-sensor communication was [4]. It assumed a network of implanted sensors and used PVs for securing the sensor communication. It did not provide sufficient detail on the PVs that could be used, but addressed the problem of removing the slight difference in PVs measured at different points in the body using an error correct approach [24]. In regards to cluster formation, [9] [26] [11] [27] [28] [10] [12] [5] [29] [30] a variety of cluster formation schemes are presented. Each of them however place considerable stress on the development of algorithms for selecting the cluster leaders while using signal signal strength based cluster formation process, making them vulnerable to attacks. In [31], a centralized cluster formation protocol which uses the base-station to decide the cluster for each node, has been described. As it is not consider security it is susceptible to sinkhole formation as well.

11. Conclusions

Security is essential for BSNs to protect the privacy of the wearer. In this paper we presented a novel means of using physiological values from the wearer's body for securing inter-sensor communication. We used this technique in two protocols for secure cluster formation in wireless wearable BSN. We further analyzed the protocols' security properties and prototyped them using Mica2 motes for testing their security using dedicated malicious sensors. The results were in accordance with our predictions in the security analysis. Our current implementation restricts itself with pre-deployed PVs, in the future we will be extending this system to enable measuring the PVs on the fly.

Acknowledgments

This research is supported in part by National Science Foundation Grant CNS-0617671 and MediServe Information Systems.

References

[1] F. Axisa, P. M. Schmitt, C. Gehin, G. Delhomme, E. McAdams, and A. Dittmar, "Flexible technologies and smart clothing for citizen medicine, home healtcare, and disease prevention," *IEEE Transactions of Information Technologies in Biomedicine*, vol. 9, no. 3, 2005.

[2] P. Lukowicz, U. Anliker, and et al., "AMON: a wearable computer for high risk patients," 2002, symposium on Wearable Computers.

[3] "Summary of HIPAA Health Insurance Probability and Accountability Act," May 2003, US Department of Health and Human Service.

[4] S. Cherukuri, K. Venkatasubramanian, and S. K. S. Gupta, "BioSec: a biometric based approach for securing communication in wireless networks of biosensors implanted in the human body," October 2003, (WiSPr'03).

[5] W. R. Heinzelmann, A. Chandrakasan, and H. Balakrishnan, "Energy-efficient communication protocols for wireless microsensor networks," 2000, in Proc. of Hawaii International Conference on System Sciences.

[6] C. Karloff and D. Wagner, "Secure routing in wireless sensor neworks: Attacks and countermeasures," July 2003, in Proceeding of IEEE International Conference on Communication.

[7] K. V. Laerhoven and H. W. Gellersen, "Spine versus porcupine: a study in distributed wearable activity recognition," Oct 2004, in Proceeding of 8th International Symposium on Wearable Computers.

[8] J. Elson, L. Girod, and D. Estrin, "Fine-grained network time synchronization using reference broadcasts," 2002, pp. 147–163, proceedings of the 5th symposium on Operating systems design and implementation.

[9] A. D. Amis and R. Prakash, "Max-min d-cluster formation in wireless ad hoc networks," March 2000, in Proceedings of IEEE Infocom Conference.

[10] S. Bandyopadhyay and E. J. Coyle, "An energy efficient hierarchical clustering algorithm for wireless sensor networks," April 2003, pp. 1713– 1723, in Proceedings IEEE Infocom.

[11] S. Basagni, "Distributed clustering for ad-hoc networks," June 1999, pp. 310–315, in Proceedings of the Symposium on Parallel Architectures Algorithms and Networks.

[12] M. Chatterjee, S. K. Das, and D. Turgut, "WCA: a weighted clustering algorithm for mobile ad hoc networks," *Journal of Cluster Computing, Special issue on Mobile Ad hoc Networking*, no. 5, pp. 193–204, 2002.

[13] R. Paradiso, G. Loriga, and N. Taccini, "A wearable health care system based on knitted integrated sensors," *IEEE Transactions of Information Technologies in Biomedicine*, vol. 9, no. 3, 2005.

[14] S. Park and R. Sivakumar, "Poster: Sink-to-sensor reliability in sensor networks," 2003, symposium on Mobile Ad-hoc Networking and Computing.

[15] A. Perrig, R. Szewczyk, V. Wen, D. Culler, and D. Tygar, "SPINS: security protocol for sensor networks," July 2001, in Proceedings of the 7th Annual ACM/IEEE International Conference on Mobile Computing and Networking.

[16] R. D. Pietro, L. V. Mancini, and A. Mei, "Random key assignment for secure wireless sensor networks," October 2003, pp. 62 – 71, in Proceedings of the ACM Workshop on Security of Ad Hoc and Sensor Networks (SASN '03).

[17] L. Eschenauer and V. D. Gligor, "A key-management scheme for distributed sensor networks," 2002, proceedings of the 9th ACM conference on Computer and Communications Security.

[18] S.-D. Bao and Y. T. Zhang, "A new symmetric cryptosystem of body area sensor networks for telemedicine," April 2005, in Proceedings of the 6th Asian-Pacific Conference on Medical and Biological Engineering.

[19] S.-D. Bao, Y. T. Zhang, and Y.-T. Zhang, "Physiological singal based entity authentication for body area sensor networks and mobile healthcare systems," September 2005, in Proceedings of the IEEE 27th Conference on Engineering in Medicine and Biology.

[20] K. Ouchi, T. Suzuki, and M. Doi, "Lifeminder: A wearable healthcare support system using user's context," 2002, in Proceeding of 22th International Conference on Distributed Computing Systems Workshops (ICDCSW'02).

[21] L. Biel, O. Pettersson, L. Philipson, and P. Wide, "Ecg analysis: A new approach in human idetification," *IEEE Transaction on Instrumentation and Measurement*, vol. 50, no. 3, pp. 808–812, June 2001.

[22] Y. Y. Gu, Y. Zhang, and Y. T. Zhang, "A novel biometric approach in human verification of ppg signals," 2003, pp. 13–14, information Technology in Biomedicine Conference.

[23] C. McWilliams, "The biophysical properties of the transdermal measurement," *International Society of Electrodermologists*, white Paper.

[24] A. Juels and M. Wattenberg, "A fuzzy commitment scheme," 1999, pp. 28–36, ACM Conference on Computer and Communications Security.

[25] D. Liu and P. Ning, "Establishing pairwise keys in distributed sensor networks," October 2003, pp. 52–61, in Proceedings of the 10th ACM Conference on Computer and Communications Security.

[26] A. D. Amis and R. Prakash, "Load balancing clusters in wireless ad hoc networks," March 2000, in Proceedings of ASSNET Conference.

[27] S. Basagni, "Distributed and mobility-adaptive clustering for multimedia support in multi-hop wireless networks," vol. 2, September 1999, pp. 889–893, in Proceedings of the Vehicular Technology Conference.

[28] D. J. Baker and A. Ephremides, "The architectural organization of a mobile radio via a distributed algorithm," *IEEE Transactions on Communications*, vol. 29, no. 11, pp. 1694–1701, 1981.

[29] A. B. McDonald and T. Zanti, "A mobility based framework for adaptive clustering in wireless ad hoc networks," *IEEE Journal on Selected Areas in Commmunications*, vol. 17, no. 8, pp. 1466–1487, Aug 1999.

[30] C. R. Lin and M. Gerla, "Adaptive clustering for mobile wireless networks," *Journal on Selected Areas in Communication*, vol. 15, no. 7, pp. 1265–1275, September 1997.

[31] W. R. Heinzelmann, "Application specific protocol architectures for wireless networks," 2000, PhD Thesis.