Author: D. B. Hoang, V. Balasubramanian and T. A. Zia

Title: Addressing the Confidentiality and Integrity of Assistive Care Loop Framework using Wireless Sensor Networks

Year: 2011

Editor: U. o. N. H. Selvaraj, Las Vegas, USA

Conference Name: IEEE International Conference on Systems Engineering (ICSENG)

Conference Location: USA

Publisher: IEEE

Date: 16-18 August 2011

Abstract: In-house healthcare monitoring applications are continuous time-critical applications often built upon Body Area Wireless Sensor Networks (BAWSNs). Our Assistive Care Loop Framework (ACLF) is an in-house healthcare application capable of monitoring the health conditions of aged/patients over a dedicated period of time, deploying the BAWSN as the monitoring component. However, the wireless medium used in the BAWSN for communications is prone to vulnerabilities that could open a door to attackers tampering with or compromising the user's data privacy. Hence, it is imperative to maintain the privacy and integrity of the data to gain the confidence and hence, the acceptance of the users of the healthcare applications. Furthermore, in time-critical applications, the vital health conditions must be monitored at regular intervals within their specified critical time. Therefore, the security model proposed for the BAWSN must not incur undue overheads when meeting the critical time requirements of the application. In this paper, we propose and implement a secure adaptive triple-key scheme (Î±TKS) for the BAWSN to achieve the privacy and integrity of the monitored data with minimal overheads. We then present the performance results of our scheme for the BAWSN, using real-time test-bed implementations and simulations.

DOI: http://dx.doi.org/10.1109/ICSEng.2011.82

URL: http://researchoutput.csu.edu.au/R/-?func=dbin-jump-full&object_id=27471&local_base=GEN01-CSU01

Author Address: tzia@csu.edu.au

Addressing the Confidentiality and Integrity of Assistive Care Loop Framework using Wireless Sensor Networks

Venki Balasubramanian and Doan B Hoang
iNEXT - Centre for Innovation in IT Services and Applications
University of Technology,
Sydney, Broadway 2007, NSW, Australia
{vsubru, dhoang}@ it.uts.edu.au

Tanveer A Zia
School of Computing and Mathematics
Charles Sturt University
NSW 2678, Australia
tzia@csu.edu.au

Abstract—**In-house healthcare monitoring applications are continuous time-critical applications often built upon Body Area Wireless Sensor Networks (BAWSNs). Our Assistive Care Loop Framework (ACLF) is an in-house healthcare application capable of monitoring the health conditions of aged/patients over a dedicated period of time by deploying the BAWSN as the monitoring component. However, the wireless medium used in the BAWSN for communications is prone to vulnerabilities that could open a door to attackers tampering with or compromising the user's data privacy. Hence, it is imperative to maintain the privacy and integrity of the data to gain the confidence and hence, the acceptance of the users of the healthcare applications. Furthermore, in time-critical applications, the vital health conditions must be monitored at regular intervals within their specified critical time. Therefore, the security model proposed for the BAWSN must not incur undue overheads when meeting the critical time requirements of the application. In this paper, we propose and implement a secure adaptive triple-key scheme (αTKS) for the BAWSN to achieve the privacy and integrity of the monitored data with minimal overheads. We then present the performance results of our scheme for the BAWSN, using real-time test-bed implementations and simulations.**

Keywords-Body Area Wireless Sensor Network; ACLF; Confidentiality; Integrity; Privacy; Healthcare

I. INTRODUCTION

The healthcare field comprises a large and growing number of ageing population and patients [2], who demand intensive resources in the provision of quality healthcare. Often, constant monitoring of the vital signs of the aged/patient is required to keep their health in check. Hospital monitoring is inconvenient for the patients and expensive for the healthcare systems. In-house healthcare monitoring systems provide a better alternative by delivering healthcare to a dispersed population through a wireless medium and the Internet. Furthermore, it would improve the quality of life of the aged and/or patients, who prefer to perform day-to-day activities in their own environments without being hospitalized. Recently, healthcare systems deploy sensors to continuously monitor the patient's vital health data to avoid any manual entry and human intervention. Consequently, the BAWSN are widely used as the monitoring component in the healthcare systems [2–5]. A BAWSN consists of wireless sensors located in the proximity of the human body, such as in day-to-day clothing or on the body as a bandage. A BAWSN is built using an underlying wireless sensor network (WSN) with a sensor to base station (aggregation point) and a base station to sensor interactions. However, the underlying Wireless Sensor Network (WSN) only constitutes a part of a BAWSN. The sensors in the BAWSN are capable of sensing the intrinsic health data of the patient and sending the data to a monitoring application in a Local Processing Unit (LPU), such as the Personal Digital Assistant (PDA) or Smartphone. The LPU receives the data for further diagnosis from the sensors through a base station.

In time-critical healthcare applications, success relies heavily on the assurance of privacy and the integrity of the data. In addition to the common network threats, the BAWSN is prone to security vulnerabilities, at the least because of their wireless medium and the lack of well-defined boundaries for such a medium. As a result, any unauthorized modification to a monitored patient's condition may induce a false diagnosis of the patient and may put the patient's life in danger. Therefore, in a healthcare monitoring application, such as the ACLF [2] that uses the BAWSN, it is essential to ensure the privacy of the patient's monitored condition through providing a confidentiality service. Similarly, the accuracy of a patient's condition must be maintained to minimise the occurrence of a life-threatening scenario. Importantly, healthcare monitoring systems are often time-critical, where the arrival of error-free health-related data to the LPU later than the expected critical time is considered as futile or unreliable [1]. Therefore, the security overhead must not add intolerable delays to the arrival period of the data and must not be the root-cause for decreasing the reliability of the system. Our Triple Key Scheme (TKS) that was earlier proposed in [8] works well for the WSN, but for time-critical applications that uses the BAWSN, the algorithm and the key management scheme of TKS should be modified to deal with the issues that are specific to BAWSN. In this paper, we propose a key-based security scheme known as an adapted TKS (αTKS), with new features, that provides high security with minimal but acceptable overheads for the BAWSN in a healthcare application, such as the ACLF. The adaptive TKS is also simple to implement.

The paper is organized into the following sections. In Section II, we briefly present the background and, Section III provides the detailed description of the security requirements for the BAWSN, the adapted TKS (αTKS), the integration of an αTKS and the BAWSN, and the analysis of the integration. In Section IV, we will demonstrate our real-time test-bed implementation and simulations that were conducted for the BAWSN's secure-key scheme and the analyses of those results. Finally, Section V will conclude this paper with a note on future work.

II. Background

Given the nature of a patient's sensitive data, it is necessary to maintain the confidentiality and integrity. This is because any illegitimate or unauthorised access to the data can be used for an illegal purpose and even a minor unauthorised alteration or fabrication to the data can lead to a life-threatening situation. In [10], the authors describe the Denial of Service (DoS) attacks and corresponding defences in the area of Wireless Body Area Networks (WBAN) with reference to the Open System Interconnection (OSI) layers. Alternatively, hardware-level encryption in sensor nodes uses a 128-bit encryption key with the help of one key per session, where a personal server shares one encryption key with all the sensor nodes in the BAWSN [13]. However, a 128-bit Message Authentication Code (MAC) can be very expensive in wireless sensor networks in terms of overheads. Interestingly, the approach proposed in [13] claims that hardware-level encryption does not significantly increase the power consumption, which is an important factor governing the deployment of wireless sensor networks. However, this claim has not been supported with any empirical or simulation results. A lightweight Identity-Based Encryption (IBE) is presented in [14] and depends on Elliptic Curve Cryptography (ECC), and therefore translates the public-key-based encryption. It has been understood in the wireless sensor networks that any public-key-based encryption is expensive [15]. Therefore, it is crucial to have a security solution that is effective, but not expensive in terms of the security overheads. Although, there is always a trade-off between the security and performance, we believe that a balance in this trade-off for wireless sensor networks can be achieved by tailoring our Triple Key Scheme (TKS) [8] for the BAWSN. This is because the design of the TKS takes into account the ad-hoc nature and resource limitations of the sensor networks that hinder the deployment of computationally expensive key management system. In the following, we briefly outline the operation of the TKS and ACLF.

A. *A Secure Triple-Key Scheme (TKS)*

The TKS consists of three keys, (a) two keys (K_n and K_s) pre-deployed at all nodes and, (b) K_c as a cluster key to deal with the hierarchical nature of the sensor network. The network key (K_n) is generated by the base station, pre-deployed at each sensor node, and shared by the entire sensor network. Nodes use this key to *encrypt* the data that is passed onto the next hop. The sensor key *(K_s)* is also generated by the base station, pre-deployed at each sensor node, and shared by the entire sensor network. Base station uses this key to *decrypt* and process the data. Also, the cluster leader uses this key to *decrypt* the data and send it to base station. The cluster key (K_c) is generated by the cluster leader, and shared by the nodes in that particular cluster. Nodes from a cluster use this key to *decrypt* the data and forward it to the cluster leader. Nodes use this key only when they are serving the purpose as a cluster leader, otherwise nodes will not need to decrypt the message received from other nodes thereby saving the energy and processing power.

Let us assume that a sensor node *A* uses K_n to encrypt the data with its ID before transmitting it to the next-hop. On receiving the data, the next-hop sensor node *B* would then forward the data to the next-hop and the process repeats until the data reaches the Cluster Leader (CL). The *CL* then uses K_c to decrypt the received data, appends its own ID and re-encrypts the modified data using its K_n. The *CL* forwards the encrypted data to the next-level CL and the process is repeated until the protected data reaches the base station. The base station then decrypts the received data using K_s and, on the other hand, uses K_n to encrypt its broadcasts. Finally, the base station verifies the decrypted message by checking the Timestamp (TS) and the ID of the sending node. In summary, these triple keys serve the purpose of confidentiality and integrity in wireless sensor networks.

To deploy the TKS in the BAWSN, these keys must be precisely tailored so that the TKS is adapted to the requirements of the healthcare monitoring system using the BAWSN.

B. *Assistive Care Loop Framework (ACLF)*

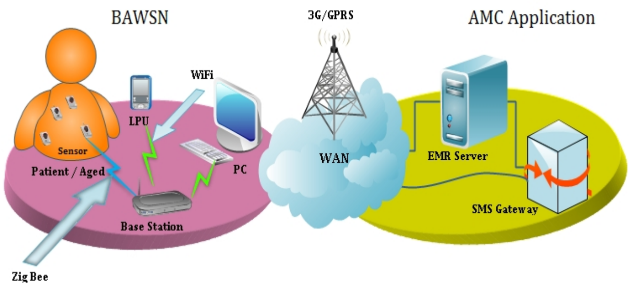


Figure 1. Assistive Care Loop Framework with BAWSN and AMC Application

As shown in Figure 1, the ACLF extends our earlier work on Assistive Maternity Care (AMC) application [2] with the BAWSN as the monitoring component. Currently, paper-based health records are maintained for pregnant women at most of the health services in New South Wales (NSW), Australia. These paper-based records have a number of disadvantages, including the poor use of space, fragility, restriction to only one user at any one time, being vulnerable to misplacement or being lost, and the effort required to conduct a search for information from either a large single record or collections of records. All these motivated us to develop an AMC application by establishing an Electronic Maternity Record (EMR). The AMC application is designed to enable medical practitioners and pregnant women to access those records from beyond the physical location of the hospital zone and, not only through desktops, but also from their PDAs. This, in turn, contributes towards the mobility and portability within the hospital environment.

In the AMC application, a pregnant woman regularly enters her Blood Pressure (BP) value using a PDA or desktop depending on the advice received from her midwife. To monitor the BP value without any manual data entry, we extended this application with the BAWSN, which is made up of a self-organized sensor, a base station and the PDA. The sensors are capable of collecting non-intrusive and intrusive health conditions of patients. The sensible and meaningful data (BP in this case) are collected and filtered using the PDA and stored in the server database, thereby creating an electronic record via the combinations of 802.15.4 (ZigBee), 802.11 (WiFi), and 3G/GPRS connections. Furthermore, depending on the gravity of the updated data, the database would notify the AMC application, which would then automatically send an alert message with specific information to the patient (or the care staff) either as an SMS or an email. A focus group for our ACLF revealed that privacy and integrity warranted attention to ensure that the ACLF was not prone to breaches. For instance, there is a necessity to ensure the sensitive information, such as blood tests for Hepatitis, HIV and issues relating to the domestic violence that were recorded on the PDAs, are not accessible to the pregnant women. This information, in the presence of third parties at home, is believed to pose confidentiality problems for the pregnant women. It is also necessary to ensure that women should not alter their information without discussions with their care provider [9].

While accessing the web-interface of our AMC application using the PDA or desktop computer, the women and care staff are provided with encrypted username/passwords. However, the PDA application, the Obi-MATE [2, 9], is a stand-alone monitoring application, whose operational authenticity is achieved by sending encrypted username/passwords as a SOAP message through the authentication module. Once authenticated, the user can then see the monitoring module in the PDA, which is coupled with the authentication module. This authentication provides the required application-level security for both the web-interface and the monitoring application. However, the same is not achieved at the message-level. Therefore, this paper focuses primarily on the message-level security for the BAWSN in the ACLF-like architecture. It is important to note that the message-level security for the wireless IP connecting the BAWSN and the AMC application is outside the scope of this paper.

III. Adaptive Triple-Key Scheme for BAWSN

As mentioned earlier, it is a pre-requisite to resolve the threats at the hop-by-hop message-level communication so that the end-to-end application-level communication can defend against those threats in the BAWSN. In the following sub-sections, we describe the message-level security requirements for the BAWSN, which is then followed by our adaptive Triple Key Scheme (αTKS) model and its deployment in the BAWSN. Finally, we conclude this section with the analysis of an αTKS using various real-time based scenarios.

A. Message-level Security requirements for BAWSN

In healthcare applications that require continuous monitoring, the arrival data rate at the LPU must be within the stipulated critical time rate. Given that the arriving data rate depends on the performance of the individual sensor nodes, a variance in any one of those sensor nodes can significantly influence the total arrival data rate [1]. This requires that all the sensor nodes in the ACLF be implemented in such a manner that they render the same data rate. For instance, a sensor node in the ACLF might have been programmed to transmit an event data every 10 seconds. In such a situation, the base station (aggregation point) is generally designed to receive all the sensed data from the sensor nodes in the High-level Data Link Control (HDLC)-like format through a serial port. Aggregated data is stored in the base station buffer, which can then be forwarded to the IP-based network or alternatively, it can be queried by the LPU. Recall that the PDA can assume the role of the LPU in the ACLF. As stated in [1], such a pull-design in a PDA requires an inequality to be programmed into the PDA to mitigate the loss of data in the base station buffer. Finally, the PDA application Obi-MATE [2, 9] completes the design by processing and filtering the collected data. Although fewer physical adversaries (as sensors are on the patient's body) can be expected in the BAWSN of the ACLF, when compared with other sensitive sensor applications (such as deployments in military-related surveillance), our study revealed that the BAWSN is constantly exposed to severe threats, at the least because of their HDLC-like data format [6,7]. In the following, we present a few scenarios that emphasise the importance of message-level security and also demonstrate how to exploit the BAWSN of the ACLF.

1. *Node Subversion:* Any captured sensor node's data would reveal its information without the need for any further processing owing to the nature of the data format used in the BAWSN. This leads to node subversion, thus implementing a confidentiality service to the data can defend against such node subversion.
2. *Passive Information Gathering:* In the ACLF systems, there is a high likelihood that more than one BAWSN may be positioned within the boundary of an AMC or other similar healthcare applications. In such a situation, an adversary may act as a base station in the vicinity and can collect the plain HDLC-like data because of the promiscuous nature of the wireless medium. Adding a confidentiality service can successfully eliminate such passive informative gathering.
3. *Node Falsification:* While monitoring more than one parameter, such as the (a) BP, (b) heart-beat rate (ECG), (c) body temperature and, (d) body mass of patient in the BAWSN, the existing setup may fall short of differentiating the semantics of the data and therefore,

may lead to the issue known as node falsification. Equally, a patient (or care staff) may implant incorrect sensors during the monitoring process that consequently leads to a false diagnosis. Note that authenticating the received information can mitigate such mistakes.

4. *Message Corruption:* The promiscuous wireless medium may open door to attackers to corrupt or modify the data transmitted by the sensors. Message corruption can be completely eliminated by introducing additional control fields that can communicate the integrity of the message.
5. *Node Malfunction:* The total arrival time at the base station would be noticeably influenced if the BAWSN experiences any node malfunction as a result of the patient (or care staff) failing to turn sensors on or if there is a break-down in any one of the sensors. Fault detection approaches can mitigate such issues.

Given that all the healthcare monitoring applications (e.g. ACLF) using the BAWSN have the above security requirements in common, we have tailored the TKS to fulfil those security requirements in the BAWSN and we refer to the tailored TKS as an *adapted TKS (αTKS)*. In other words, the αTKS is designed to deliver the following objectives, (i) meet the security requirements of the BAWSN, (ii) ensure that sensors consume less computation power for their security operations, (iii) minimize the overhead, (iv) permit application developers to have control over the implementation and, (v) resolve attacks that are specific to the sensor networks. The following sub-sections describe the model and implementation of an αTKS in the BAWSN.

B. *αTKS Model*

Recall that in the BAWSN, the PDA acts as the LPU and also serves as the connector between the BAWSN and the AMC application. Alternatively, the base station serves as the connector for any extended Wireless Sensor Networks (WSNs). In comparison, the base station in the BAWSN assumes the role of a cluster head and, unlike the WSN; the BAWSN consists of only one cluster head that is connected directly to the PDA. Because this paper focuses on only securing the BAWSN, the PDA (or the LPU) is considered as the end-point for the BAWSN. Remember that in the ACLF, the PDA pulls the data that is sent to the base station by the sensor nodes for further processing. Therefore, it is necessary to encrypt the data that is transferred from the sensor-to-base station and then from the base station-to-PDA.

The network key (K_n) is programmed into both the sensors and the base station using nesC [7], a C-based programming language for the networked embedded systems. The sensor nodes in the BAWSN are designed to send the data only to the designated base station and therefore, the sensor nodes boycott any data designated to them. Alternatively, these sensor nodes can route the data designated to the base station. In other words, such a boycott or redirection can mitigate the packet floods that may otherwise impact the network resource and performance. Hence, these sensor nodes are not equipped with any decryption key, thereby eliminating the need for data processing. The base station is programmed with the cluster key (K_c) so that it can decrypt the data received from the sensor nodes and the PDA is programmed with the sensor key (K_s) and can decrypt the data received from the base station (as shown in Figure 2).

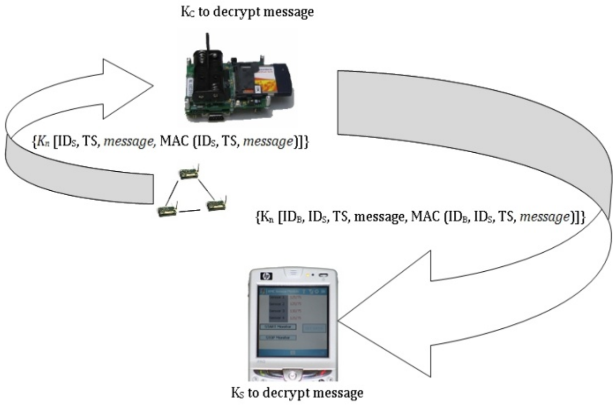

Kc to decrypt message
{Kn [IDS, TS, message, MAC (IDS, TS, message)]}
{Kn [IDB, IDS, TS, message, MAC (IDB, IDS, TS, message)]}
KS to decrypt message

Figure 2. Implementation of αTKS in BAWSN components

1) Sensor Node Key Calculation: For instance, when a sensor node (ID_S) sends the data to the base station, it constructs the data using the actual message together with the pre-deployed Message Authentication Code (MAC) and the current timestamp (TS) as follows:

ID_S →Base Station: {K_n [ID_S, TS, message, MAC (ID_S, TS, message)]}

Note that the data sent from the sensor node to the base station is encrypted using the network key (K_n).

2) Base Station Key Calculation: The base station uses the cluster key (K_c) to decrypt the data received from the sensor node. First, the base station checks the identity of the sensor node, i.e. using the ID_S contained in the data and second, verifies the authenticity and integrity of the data through the MAC. Any mismatch would cause the base station to drop the data. The base station then encrypts the authenticated data using the network key (K_n) along with its identity (ID_B). As shown below, the newly encrypted data is then placed in the base station buffer for the collection by the PDA.

ID_B → PDA: {K_n [ID_B, ID_S, TS, message, MAC (ID_B, ID_S, TS, message)]}

3) LPU/PDA Key Calculation: When the PDA retrieves the data from the base station at regular intervals, it decrypts the data using the sensor key (K_s). Initially, the PDA checks the identity from the data and then verifies the authenticity and integrity of the data through the attached MAC. In addition, the PDA also checks the identity of the sensor nodes (for example, ID_S) in the decrypted data and should any of those identities mismatch, it drops the acquired data.

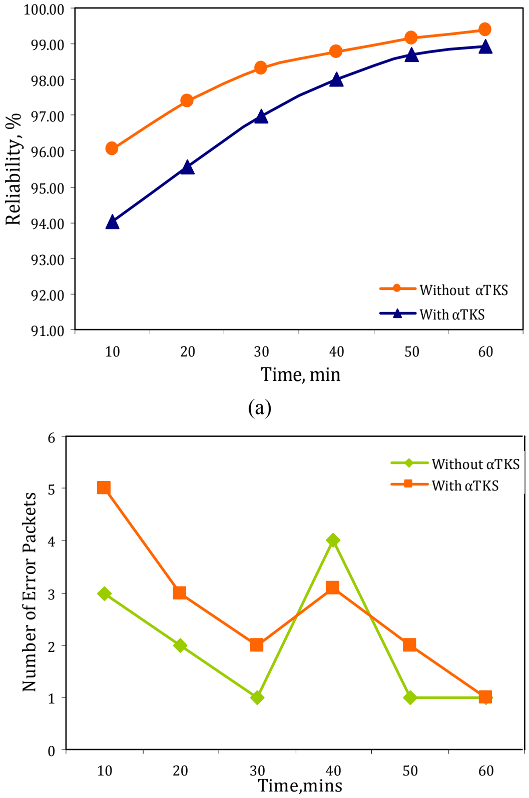
IV. Performance of Adaptive TKS in BAWSN

We conducted both test-bed implementation and simulations to study the performance of the BAWSN in the presence of an αTKS. We had shown in [8, 17] that the TKS performs better than the well-known security schemes, such as, TinySec [15] and MiniSec [16]. Our empirical studies compare the behaviour of the BAWSN with and without an αTKS.

A. Test-bed Implementation

As mentioned-earlier, our BAWSN includes heterogeneous components that not only differ in terms of processing power and storage capacity, but also are divergent in terms of the operating platforms. The sensor components consist of four Crossbow-technology-based mote sensors [2,6] that operate using the TinyOS [7]. These motes are made up of a MICAz processor and radio platform integrated together with a sensor board. Here, the sensor board is a single hardware; Crossbow produces different types of sensor boards capable of sensing light, temperature, heart rate, arterial pressure etc. Hereafter, we implicitly denote Crossbow motes that are plugged-in with the required sensor board as sensor motes. Given that the end-point in our scenario is the LPU, a PDA is generally connected with a Stargate gateway [1,2], which acts as the base station and interconnects the 802.15.4/ZigBee-based Crossbow family motes and the 802.11-based PDAs. Note that the Stargate can be used as a base station only after housing a base mote sensor on the Stargate board [6]. Stargate is programmed using a C-based application called SerialForwarder that is provided by the TinyOS. A serial port is used by the Stargate to contact the sensor mote and in that case, the SerialForwarder is used to read/send packets from/to the serial port. Alternatively, the Stargate is reachable from a PDA by connecting the PDA through 802.11 in the *ad-hoc* mode. As shown in Figure 3(a), the impact of an αTKS was measured by computing the average of the series of real-time experiments that had identical set ups and parameters. In our ACLF, each of these experiments ran for a period of 60 minutes. The reliability of the BAWSN (with and without an αTKS) was measured, based on our *reliability measurement model* [1] that takes into account, (a) the data that were lost as a result of the base station buffer overflow, (b) received error-prone data and, (c) the delay in the data arrival time.

Although, the reliability of the BAWSN with an αTKS is marginally lower than the reliability realized in a BAWSN without an αTKS, our experiments revealed that both cases realize a gradual reduction in the packet loss at the base station buffer owing to the inequality programmed into the PDA [1]. In both scenarios, a significant improvement in the reliability can be observed at the beginning and then a marginal improvement as time proceeds. Interestingly, the reliability of the BAWSN with an αTKS narrowed the difference with its counterpart when the experiments reached their maximum time limit. As discussed in [1], the inequality design may facilitate achieving a negligible data loss because of the buffer overflow. In such a situation, the reliability of the BAWSN then depends only on the error-prone data and the delay in the data arrival time. As shown in Figure 3(b), it is important to note that the increase in the data size owing to an αTKS failed to contribute towards an error packet, because this can occur in any wireless sensor network as a result of the various factors stated in [1]. In summary, the addition of an αTKS minimally decreases the reliability because of the delay in the packet arrival that resulted from the augmented computational time to encrypt/decrypt data at various levels; but on the other hand, the same operation extensively improves the security of the BAWSN.



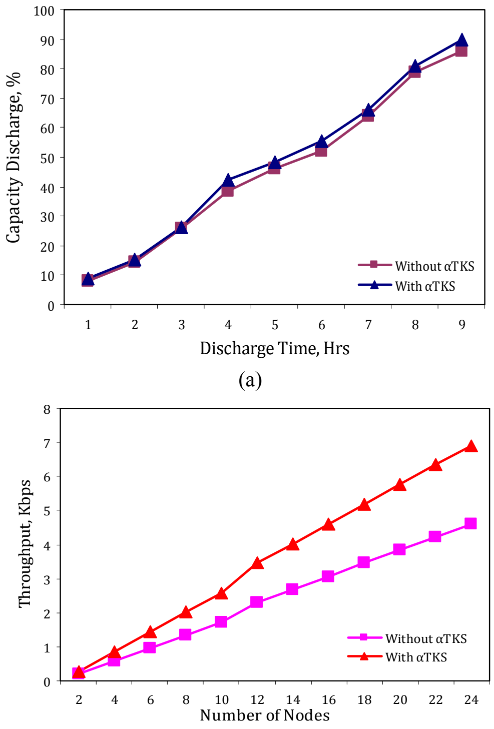
(a)

(b)

Figure 3. Performance of BAWSN with and without αTKS, (a) Operational Reliability (b) Packet Error

B. Simulation Results

To study the performance of the power consumption resulting from the increase in the packet size and also to investigate the behaviour of the BAWSN in the presence of more than four mote sensor nodes, we have simulated a BAWSN that ranges from two sensor nodes to 24 sensor nodes using the j-sim [14]. The j-sim has extended the notion of network emulation to motes-based WSNs. The extended module has Berkeley motes, equipped with sensors and RF circuitry, and is used as the real devices to extract the required data. A sensor node also has a power model that embodies the energy-producing components (battery) and the energy-consuming components (radio and CPU).



(a)

(b)

Figure 4. Performance of BAWSN with and without αTKS, (a) Battery Discharge (b) Throughput

Figure 4(b) presents the overhead at the sensor nodes (with and without an αTKS). Here the throughput is seen as the total amount of data received from the sensors in a BAWSN. Although, it is unlikely that a BAWSN may use more than six sensor nodes for any given single parameter (BP in our case) the overhead of data with an αTKS would always be less than 570 bits (security overhead: bits x number of sensor nodes). It is important to note that this overhead has a minimal impact on the processing power of the sensors (Figure 4(a)). Furthermore, it can be seen from Figure 4(a) that the discharge rate of the battery is almost identical for both the cases.

V. Conclusion

Body area wireless sensor networks (BAWSN) have been increasingly deployed for monitoring the health and wellbeing of vulnerable individuals. The acceptance of sensor-based services depends heavily on their ability to maintain the privacy and security of the monitored data with little overheads and acceptable costs. As sensor nodes have limited resources in terms of energy, memory and processing, security solutions for sensor networks have to be realistic with minimum overheads and do not incur excessive penalty on the performance of the whole monitoring system. In this paper we have presented the deployment of an adaptive secure triple-key scheme (αTKS) in a BAWSN to ensure the Confidentiality and Integrity of the data collected with minimum overheads. Our experimental results show that the deployment of an αTKS does not affect the performance of BAWSN; in fact, it achieves a significant level of security with a very minimal trade off.

References

[1] Venki Balasubramanian, and Hoang, D.B. 2010. “Reliability Measure Model for Assistive Care Loop Framework using Wireless Sensor Networks.” International Journal of Healthcare Engineering, 2010, 1(2), 239–254.

[2] Venki Balasubramanian, and Hoang, D.B., 2008. “SOAP-based Assistive Care Loop using Wireless Sensor Networks.” Proceedings of the 1st IEEE International Symposium on IT in Medicine and Education, Xiamen, China, 409–414.

[3] Jovanov, E., Raskovic D., Price J., Chapman J., Moore A., and Krishnamurthy A. 2001. Patient Monitoring Using Personal Area Networks Of Wireless Intelligent Sensors, Biomedical Sciences Instrumentation, 37, 373–378.

[4] Wilson L.S., Gill R., Sharp I.F., Joseph J., Heitmann S. A., Chen C.F., Dadd M.J., Kajan A., Collings A.F., and Gunaratnam M. 2000. “Building The Hospital Without Walls – A CSIRO Home Telecare Initiative.” Telemedicine Journal, 6(2), 275–281.

[5] Harvard University. CodeBlue Project: Wireless Sensor Networks for Medical Care. 2010. http://fiji.eecs.harvard.edu/CodeBlue [accessed 24 January 2010].

[6] Crossbow Technology Inc., Motes, Wearable Sensors. 2004. http://www.xbow.com/ [accessed 24 January 2010].

[7] TinyOS Embedded Operating System. 2010. http://www.tinyos.net [accessed 24 January 2010].

[8] Zia, T. A. and Zomaya, A. Y. 2006. “A Secure Triple-Key Management Scheme for Wireless Sensor Networks”. In the proceedings of the IEEE INFOCOM 2006 Students Workshop, 23–24 April, Barcelona, Spain

[9] Homer, C., Christine, J.C., Ahmad, N.F, Venki Balasubramanian, Hoang, D.B., Lawrence, E., Foureur, M., and Leap, N. “Developing an interactive electronic maternity record.” British Journal of Midwifery (Accepted for publication).

[10] Saleem, S., Ullah, S., and Yoo, H. S. “On the Security Issues in Wireless Body Area Networks.” 2009. JDCTA: International Journal of Digital Content Technology and its Applications, Vol. 3, No. 3, pp. 178–184, 2009.

[11] Warren, S., Lebak, J., Yao, J., Creekmore, J., Milenkovic, A., and Jovanov, E. 2005. “Interoperability and Security in Wireless Body Area Network Infrastructures.” Proceedings of the 27th Annual IEEE Conference on Engineering in Medicine and Biology, 1–4 September 2005. Shanghai, China.

[12] Tan, C. C., Wang, H., Zhong, S., and Li, Q. 2008. “Body Sensor Network Security: An Identity-Based Cryptography Approach.” First ACM Conference on Wireless Network Security (WiSec’08), 31March–2 April 2008. Alexandria, Virgenia, USA.

[13] Prasad, N. R., and Alam, M. 2006. “Security Framework for Wireless Sensor Networks.” Journal of Wireless Personal Communications 37:455–469. Springer Netherlands.

[14] Ahmed, S., Wei-Peng, C., Jennifer, C. H., Lu-Chun, K., Ning, L., Hyuk, L., Hung-Ying, T., and Honghai, Z., 2005. “J-Sim: A Simulation Environment for Wireless Sensor Networks”, Proceedings of the 38th Annual Simulation Symposium, San Diego, USA.

[15] Karlof, C., Shastry, N., and Wagner, D. 2004. “TinySec: A Link layer Security Architecture for Wireless Sensor Networks.” SenSys’04, 3–5 November 2004, Baltimore, Maryland, USA.

[16] Luk, M., Mezzour, G., Perrig, A., and Gligor, V. 2007. “MiniSec: a Secure Sensor Network Communication Architecture.” In Proceedings of IPSN’07, 25–27April, Cambridge, Massachusetts, USA.

[17] Zia, T. A., and Zomaya, A. Y. 2010. Quality of Security (QoSec) through Triple Key Scheme in Wireless Sensor Networks, Wiley Interscience Journal of Wireless Communications and Mobile Computing. Vol. 10, Issue 5, pp. 722-732.