A Review of Physical Attacks and Trusted Platforms in Wireless Sensor Networks

A.M.Bharath Kumar
Asst.Professor,Dept of ECE,Krishna chaitanya Institute of Technology and Science,
Markapur,Prakasam(Dist),Ap,India.

Abstract— **Wireless Sensor Networks (WSNs) have shown great promise as the emerging technology for data gathering from unattended or hostile environment. The advancement in micro-electro-mechanical sensor technology, wireless communication technology and the recent energy scavenging have greatly contributed to the widespread acceptance of WSN related applications. In addition, the design of sensors that are small, low cost, low power and combined with its ability to be left unattended has made it more viable and indirectly promotes its popularity for future solutions in various real-life challenges. However, in sensor network, the nodes are physically accessible by adversaries and have been known to expose cryptographic materials such as the encryption keys and other important data in the sensor nodes. Acknowledging the severity of such attacks, this paper first presents the review on physical attacks followed by the introduction of trusted platform with protected memory that not only protect sensor node's sensitive credentials but also provide a concrete way to trust nodes in the dedicated wireless sensor network. Finally, summarization of proposed IBE_Trust framework is presented and briefly discussed.**

Keywords— Wireless Sensor Networks, Physical attacks, trusted platform, security

1.Introduction

Wireless Sensor Networks (WSNs) normally consists of a large number of distributed nodes with sensors, embedded processor and low power radio for wireless communication with each other and with the base station. While sensor nodes perform specific task at the intended location, the base station which is a more powerful device, act as a front-end to WSN users hence offering the functionality of sensory mechanisms for the computer systems. Furthermore, the benefits of using WSNs technology is undeniable which includes simple and inexpensive deployment due to the use of wireless interface, the ability to be left unattended and longer surviving time. The range of potential applications that WSNs may offer is tremendous ranging from basic temperature measurement to complex applications. Such applications include personal sensing [6], body area network [8, 9], military [10], smart building [11], camera and video surveillance [12] as well as robotics [13]. It is believed that, advancement in sensor technology, wireless communication technology and the network technology has greatly contributed to the widespread adoption of WSNs applications in today's and future way of life. However, as the demand for WSNs related application increases, the security and trust issues are no longer can be treated as extra services or supplementary entity. These security issues should be considered and addressed during the system development to ensure widespread public acceptance. In addition, the distributed and randomly deployed nature of these sensor nodes at remote areas makes them vulnerable to numerous security threats. More seriously, the security breach can result in physical side effects, personal injury, and even death. Unfortunately, WSNs have unique constraints as compared to traditional networks, rendering the existing security measures implemented for wired or wireless communication network impracticable. These constraints are basically due to the limitations on the sensor nodes' memory, energy, processing power and the ad hoc wireless channel used. To adhere to the constraints faced by sensor nodes, the security scheme should be carefully designed and should be based on the intended applications and be aware of the possible threats to the applications. In other words, the security scheme should be developed after identifying the type and nature of the intended applications. In general, security is commonly referred as data authenticity, integrity and confidentiality. Good amount of research in this area are mostly focused on energy efficient security algorithm [14-21] to ensure minimum energy is utilized to achieve the above security features. However, the demand to exchange information between trusted sensor nodes is also a must and is widely covers in Trust Management Systems [22-24]. Recently, great progress has been accomplished in providing the basis for energy efficient trusted platform. Among the commercial releases are Trusted

Platform Module[25], ARM1176JZF-s with TrustZone [26] and TI M-Shield[27]. The recent development that incorporate the above security chips are TrustFleck [28], TrustCAM[29], SEF[30] and IBE_Trust[31]. This paper provides a clear picture on the demand of trusted sensor node by first considering the types of physical attacks by means of physical tampering and followed by review of implementations related to trusted sensor node in the WSN area.

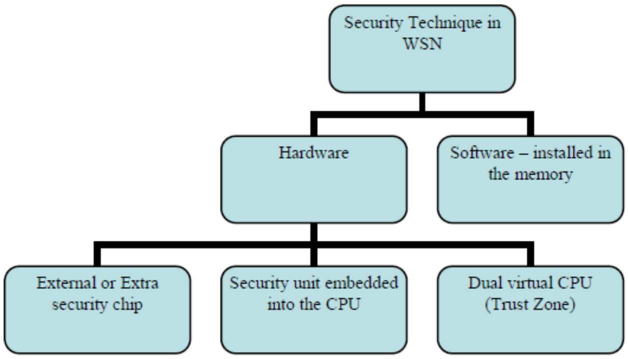

Security Technique in WSN
Hardware
Software – installed in the memory
External or Extra security chip
Security unit embedded into the CPU
Dual virtual CPU (Trust Zone)

Fig.1: Security Implementation Technique in WSNs.

In software implementation, researchers look for simplified algorithms that offer similar or higher security level but overcome constraints in the sensor node. While a good number of research are focused on developing the most suitable cryptography algorithm for sensor node , architectures in the sensor node. This work is basically prompted from the study that shows better performance of sensor network security for hardware implementation.

2.Physical Attacks

Before focusing on the physical attack, it is good to have a general overview on the factors that create security demand in WSNs. Threats, vulnerabilities and attacks are three crossly related entities that usually caused havoc to the security of the information owned by others. Threat is basically an ability or intention of any agent to adversely affect the operation, system or facility offered by that network and can be categorized as amateur, professional and well-funded adversary. Amateur types of attacks include denial-of-services or eavesdropping through wireless sniffing. A professional type of adversary on the other hand, usually launches more sophisticated attacks such as hijacking, man-in-the middle or Sybil attack. Finally a well-funded adversary with highly sophisticated tools will launch attacks such as node capture, wormhole or rushing attacks [32]. Subsequently, vulnerabilities are defined as anything that leaves an information system open for potential exploitation. The nature of WSNs itself such as physical limitation, wireless communication and unattended nature can be said as major sources of vulnerabilities to WSNs applications. Finally, attack is best described as an action with an intention to bypass the security control of the system and is further classified into passive and active attacks. The physical type of active attacks can be performed by insiders or outsiders. Due to space limitation, the following paragraph will only focus on physical types of attack. Relationship between threats, vulnerabilities and attacks can be portrayed as in Fig. 1 and is explained as, “Threats that come from various background and identities and with different intentions will generate various types of attacks to tamper or steal the valuable information from the valuable entity. In addition, successful attacks are very much dependent on the vulnerabilities surrounding the valuable entity, which is referring to the sensor node in this case”. Physical attacks can be broadly defined as attacks that involve direct physical access by adversary to the sensor node. Usually after capturing the node, the adversary proceeds to tamper or extract the confidential data before redeploying the node into the network. Therefore, the effect of node capture attack is categorized as hazardous by [33] because it can lead to various data exposure, clone node and other various types of attacks. Roosta et al. [34] have divided physical attacks into two classes which are *invasive* and *non-invasive* attacks. Invasive attacks require sophisticated tools on or away from the site while the non-invasive is usually attacked through JTAG port that is widely used during the development and debugging phase. In other words, enabling the JTAG port adds another vulnerability to the system. Mostly invasive attacks happen through the physical capture of the sensor node. While preventing node capture in large distributed WSNs deployment area is almost impossible, the focus should be on securing the confidential data in the sensor node. Currently, as listed in Table 1, there is no practical solution, based on the cited papers only, available to make the sensor nodes resistant to physical tampering. The related micro-controller for the sensor nodes lack or do not mentioned in the paper the hardware-based memory protection features.

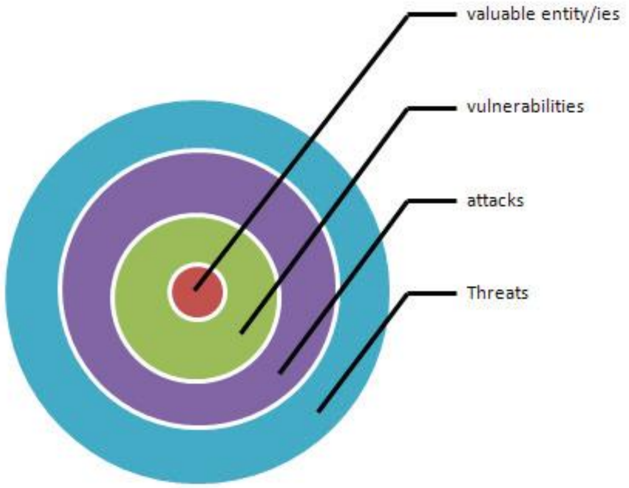
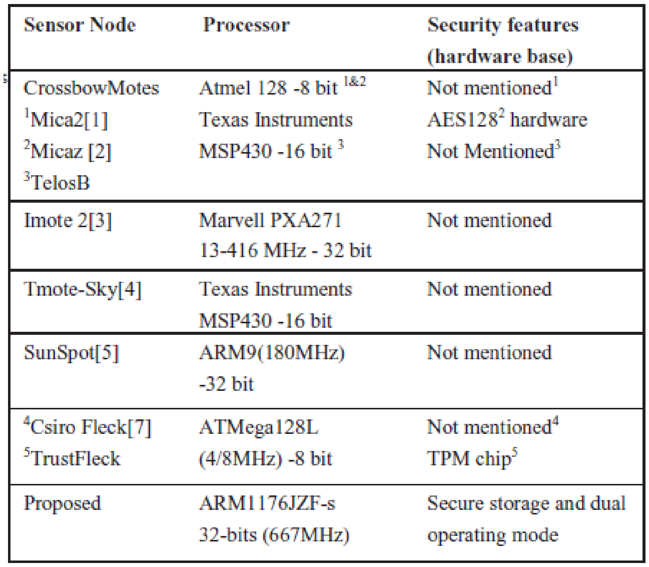


Fig 2. Threats, attacks and vulnerabilities (TAV)

Table 1. Sensor nodes security features



Sensor Node	Processor	Security features (hardware base)
CrossbowMotes [1]Mica2[1] [2]Micaz [2] [3]TelosB	Atmel 128 -8 bit [1&2] Texas Instruments MSP430 -16 bit [3]	Not mentioned[1] AES128[2] hardware Not Mentioned[3]
Imote 2[3]	Marvell PXA271 13-416 MHz - 32 bit	Not mentioned
Tmote-Sky[4]	Texas Instruments MSP430 -16 bit	Not mentioned
SunSpot[5]	ARM9(180MHz) -32 bit	Not mentioned
[4]Csiro Fleck[7] [5]TrustFleck	ATMega128L (4/8MHz) -8 bit	Not mentioned[4] TPM chip[5]
Proposed	ARM1176JZF-s 32-bits (667MHz)	Secure storage and dual operating mode

Non-invasive attacks, such as side-channel attacks, are also possible in sensor networks. For example, a study by [35,36] have shown that side-channel attacks can be launched by taping the signal from the chip and using simple power analysis as well as differential power analysis to reconstruct the data. Their results suggest the possibilities of extracting several key bits through the power analysis attack. Another form of non-invasive physical attack is by exploiting the Bootstrap Loader (BSL) and happens mostly during the boot up process. By having access to the boot devices and debug session, attackers will be able to analyze the systems and its operation thus providing them with enough information to clone the system, insert malware and disturb the overall operations of the sensor node and its systems [37, 38]. More recently, over-the-air programming has been employed for remote software update. Although it has been found useful for researchers and network owners, the procedure generally leaves the door "wide open" for injection of malicious code. Even though it is hardly done due to Harvard architecture type of memory, Francillon [38] in his work has successfully injected malicious code in Micaz class motes thus triggering the alarm for the need of holistic security scheme for wireless sensor network. Another interesting work reported by [39] further classifying the attacks into semi-invasive attacks. Semi-invasive attacks require repackaging of the processor to get access to its internal layer. However, no electrical contact is required as compared to invasive attacks and therefore represents greater threat to the hardware based security. The researcher in his work has successfully performed fault injection attacks to modify memory content and also extract data from powered-off memory devices. In can be concluded that the intention of the physical types of attacks can vary from destroying the sensor node, extracting confidential data and finally to being falsely authenticated or authorized in the network. Successful physical attacks will usually leads to node cloning attack and therefore create another demand to differentiate between cloned and genuine node in the network. Today, in embedded systems, crypto-processors or physically secure processors have been used extensively to provide some level of resistance to physical tampering. Even though attacks on crypto-processors are known to occur, they still provide the first line of defence against physical tampering. Therefore, optimizing crypto-processors to fit the low-cost, lowenergy requirements of sensor networks can play a significant role in raising the security level. Subsequent section will briefly discuss on the available and possible security chips to address the above physical tampering issues in WSN.

3. Physical Attack Mitigation

It is believed that security chip with on-SOC memory and with extra security features can help in lowering done the risk of exposing sensor node sensitive credentials due to physical tampering. Among current commercially available low energy embedded security module are the Trusted Platform Module (TPM) by Atmel, ARM11 with TrustZone by ARM and latest TI-M Shield by Texas Instrument. Basically the TPM offers the foundation for a trusted platform. It can be added to existing architecture such as SecFleck sensor node, hence providing the lowest layer for larger security architecture. TPM verifies the integrity of systems through trusted boot, strong process isolation and remote attestation that verifies the authenticity of the platform. On the other hand ARM1176JZF-s with TrustZone features consist of hardware enforced security processor providing code isolation and two separated parallel execution world which are secure and non-secure. In addition, it also offer basic security services such as crypto engine and On-SoC memory for safety storage and integrity checking to help ensure device and platform security. Another, TI M-shield, a system-level security solution specifically designed for securing wireless mobile applications. TI M-Shield is designed with the intention to provide hardware solution for widespread adoption of new mobile services and the convergence between mobile and internet services. Like the ARM1176JZF-s processor, TI M-Shield also comes with embedded security and TrustZone features and most importantly, the hardware security solutions complies with basic trusted environment standard. As of now, the successful implementation of trusted sensor node, utilizes the TPM chip as the security chip. However, both work (Trustfleck and SEF) incorporate TPM chip into the sensor node platform resulting in bigger sensor node size. Another, TPM chip was basically designed for personal computer and therefore contains superfluous commands for basic security processes which later lead to higher energy consumption. Conversely, ARM11 and TI M-Shield although designed with low energy consumption, the use of both processors especially in the research area are limited due to the proprietary issue.

4. Trusted Sensor Node

According to [40], trust is establish when an entity always behaves in an expected way for any intended functions. Another, Javier et al. [23] define trust as an important tool that can solve one of the intrinsic problems of WSNs which is the uncertainty in collaboration. In WSNs environment, it is usual for sensor nodes to be deployed in unsafe locations and being left unattended for considerable long periods of time. After being implemented for a length of time, some of the nodes may need to be replaced when they are malfunctioning, found missing, or when their battery has exhausted. Also, new nodes may be deployed in order to enhance network's capability or to increase network's coverage. Further, the old and new WSNs node members need to collaborate with each other in order to provide services to the network or to execute their specific task. As an example, in order to forward data to base station, nodes may have to send its data to neighbouring node and most of the time, nodes act as a router forwarding packet to BS. It is highly important that the collaboration exist is between two trusted entities. Unfortunately, few works on trust in WSNs such as Roosta [34] and Tanveer [41] assume a trustworthy base station and no trust at all for the sensor node. Therefore, ensuring that only authenticated and trusted nodes exist in the networks is essential in avoiding any other entities interfering in the network operations. Based on previous implementation in WSNs, trust was established through Trust Management System (TMS) and Trusted Platform Module (TPM) crypto-processor chip that is based on Trusted Computing Group (TCG) specifications. From authors' point of view, trust according to TCG is better as regarded to TMS. This is mainly due to the method used to establish the trust relationship or status where in TCG the trust is by mean of concrete stages while in TMS, trust status of nodes are dependent on their neighbours assumptions or point of view. Therefore, subsequent section will only concentrate on trust according to TCG.

4.1. Trusted Computing Group (TCG)

Trusted Computing Platform Alliance (TCPA) was formed in late 90's with the mission to implement trust into client, server, networking, and communication platforms and it finally emerged as TCG in 2003 [42]. TCG basically worked to develop an inexpensive chip that helps users protect their sensitive information. TCG used secure hardware Trusted Platform Module (TPM) chip as a basis for trusted computing that provides a level of relevant since hardware based security is difficult to compromise than conventional approaches. TPM verifies the integrity of systems through trusted boot, strong process isolation and remote attestation that verifies the authenticity of the platform. Encryption and decryption are done using the Rivest, Shamir and Adleman (RSA) algorithm with default 2048-bit, SHA-1 hash, and random key generator. TPM can be implemented in a dedicated chip, co-processor or can be software-based [31]. However, the connection of TPM is vendor specific and is not specified by TCG [28]. Trust in TCG is evidence based and is categorized into three processes; *properties*, *measurement* and *reporting or attestation.* The evidence which is the outcomes from the process will provide sufficient identification to those wishing to trust the platform. In WSN, this evidence mechanism is very useful as it can provide a solid value or method to

BS to trust newly joining nodes or nodes that re-joins the network. Moreover, the design which is based on trusted computing ensures better protection against previously discussed physical type of attacks. Fig. 3 depicts the concrete chain-of-trust for trust establishment in TCG and in proposed work.

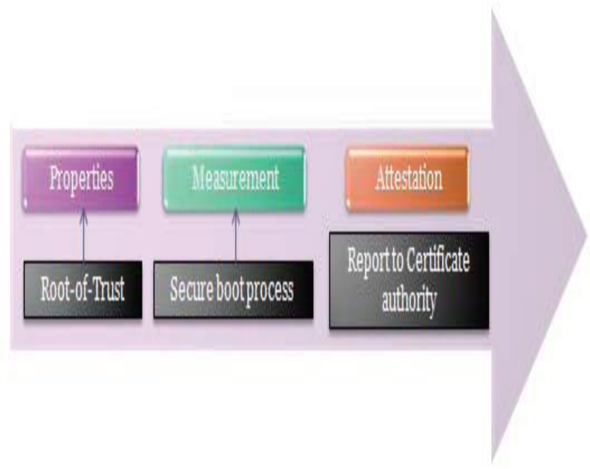


Fig. 3. Concrete Trust Process

4.2. Related works in trusted WSN

This section provides brief overview of the directly relevant trusted wireless sensor node platform by focussing on the trust establishment according to the TCG specifications in WSNs. SecFleck [43] and latest renamed as Trustedfleck [44], used external TPM chip on the sensor node. This TPM based public key platform facilitates message security services with confidentiality, authenticity and integrity. SecFleck platform consists of hardware and software module and later connects to the Fleck [7] sensor node board. Although the evaluation on the computation time, energy consumption, memory footprint and cost is reasonable and positive, the extra platform connected to the sensor node is seemed to be unpractical for sensor node applications. Besides, there are superfluous TPM commands required in performing its functions, in which both contribute to higher energy utilizations. Another two studies have embarked on the development of trusted and secure platform utilizing ARM11 trust zone architecture. Johannes Winter[45] and Xu Yang-ling[46], both utilize Linux kernel 2.6 and ARM TrustZone features. While Johannes merge TrustZone features with TCG-style trusted computing concepts in Mobile Trusted Module (MTM), Xu integrate the Mandatory Access Control (MAC) in Linux kernel 2.6 with the TrustZone features to enhance the security up to the non-secure environment. The first has designed a robust and portable virtualization framework for handling nonsecure guest while the second work presented an embedded system security solution. However, constraints on resources were not considered in the design those limit its applicability to embedded appliances such as in mobile applications only. Latest, Song Wen et al. present framework of trusted sensor network based on Trusted Computing concept utilizing TinyPK [47] protocol. Their framework consists of Trusted Computing Based (TCB) and an effective trust chain to form a complete trusted WSN platform. TinyPK on the other hand is a public key based protocol using ECC algorithm that have been proven to provide equal security level as RSA algorithm, but with lower security bits make suitable and practical for WSN environment. The root of trust in this framework is the trusted server that acts as a certification authority (CA). Based on the hierarchal architecture, the cluster head nodes will first join the network by authenticating themselves with CA. Sensor nodes that were pre-deployed with network information such as node identification, CA's public key, node's public and private key and signed public key will then joined the network by authenticating themselves with CA or cluster heads in the network. However, this work utilized public key concept that have extra communication during key establishment.

5. Framework of IBE_Trust

The main reason towards the development of this framework is to provide a concrete method in ensuring a node's trustworthiness prior to joining the network. TCG's specification in trust establishment has been chosen as the guideline due to its standard procedure. This work is based on the principle that effect to attacks on sensor node can be reduced through platform security enhancement. As such a framework called IBE_Trust is proposed by the authors to achieve this objective. Two main components involved in the development of the framework of trusted wireless sensor node are generation of platform unique entity and IBE-Trust protocol. While the first prevents duplication of node's identity, the second acts as an access control scheme to protect sensor network from invalid sensor node. Due to limited space, a summarized analysis on the performance of proposed IBE_Trust protocol compared to previous implementations that utilized different cryptography algorithm during authentication process is depicted in Fig. 3. IBE_Trust which is based on Tate-pairing algorithm [48] and which utilizes identity-based cryptosystem performs much better compared to

RSA-1024 but performs slightly poorly compared to ECC- 160 works. The values represent percentage energy used in the implementation of two processes which are: i) client or sensor node sending encrypted data to server or base station for authentication purposes and ii) acknowledgement/s from the server to client for authentication purposes. Power measured includes processes such as encryption, decryption, generation of public key in IBE_Trust, transmitting and receiving packets. For communication between client and server, IBE_Trust report higher energy percentage compared to ECC. This is basically due to the secure boot process during node first booting up and therefore considered as reasonable. For server to client, IBE_Trust report lower energy utilization. Finally, results proved feasibility of proposed framework in term of energy utilization in the WSNs environment. Details analysis on the framework is however available in [31].

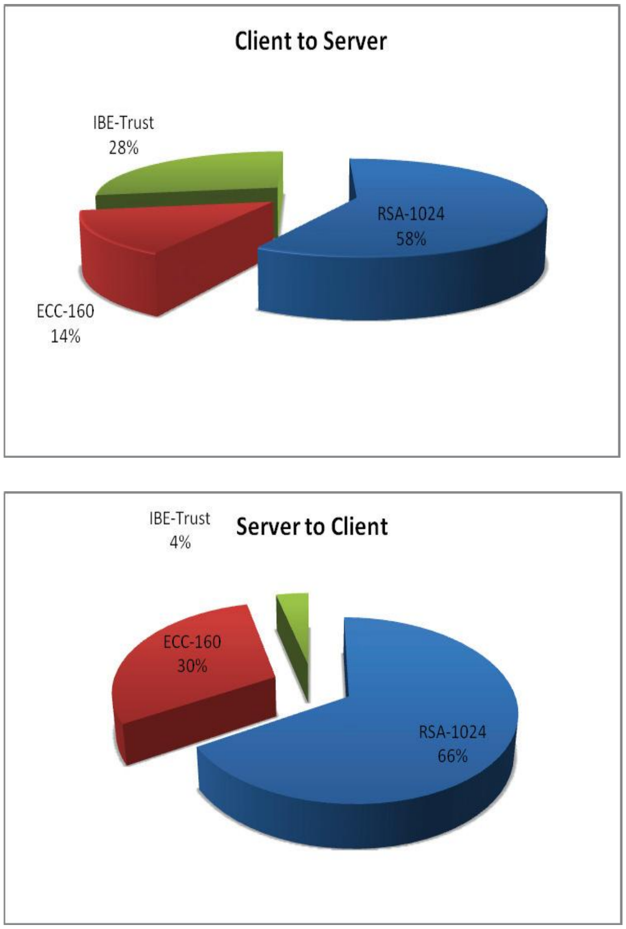


Fig.3. Power consumption during the authentication process

Utilizing ARM1176JZF-S as the processor with its on-Soc memory has helped the proposed framework to protect important credentials such as sensor node private keys. Moreover, in this scheme, only part of the private key is stored in the sensor node memory thus further protecting the network since the disclosure of part of the private key will not lead to exposure of encrypted data. Moreover, images such as encryption and decryption are stored in the secured memory region of flash memory and are only accessible in the secured mode environment. The effect of BSL attacks can also be reduced through the secure boot process where the integrity of images loaded has been verified to prevent sensor nodes from running malicious code. Through the proposed framework, node impersonation has also been prevented. Node impersonation happens when intruders manage to duplicate the unique identity of the sensor node that is being used during authentication. Identification of masquerading nodes through their inability to regenerate the exact trust value required through its boot process has significantly reduced the possibility of having a masquerade node joining the network and subsequently launching node cloning attacks.

6. Conclusion

This paper has presented a review of the types of physical attacks on sensor nodes and of various trusted wireless sensor platform. This paper contributes to the general model on the relationships between threats, attacks and vulnerabilities in the area of WSNs. This was followed by a discussion on physical types of attacks that contribute to a better understanding of the capabilities of different classes of physical attacks and their possible consequences. To reduce the effect of physical attacks on sensor nodes, the use of embedded security chip in the sensor node is proposed. Finally, this paper looked at the related work on trusted sensor node and presented a brief analysis on proposed work. It can be concluded that, further research on trusted sensor node with hardware based security is essential to provide enough security for more challenging future applications of WSNs.

References

[1]"Mica2,"https://www.eol.ucar.edu/rtf/facilities/isa/internal/CrossBow/DataSheets/mica2.pdf, [11 May 2011].

[2]"MICAz,"http://www.openautomation.net/uploadsproductos/micaz_datasheet.pdf, [11 May 2011].

[3] "Imote2," www.memsic.com/support, [11 May 2011].

[4"Tmotesky,"http://www.bandwavetech.com/download/tmote-sky-datasheet.pdf, [11 May 2011].

[5]"SunSpot,"http://www.sunspotworld.com/docs/Yellow/eSPOT8ds.pdf, [11 May 2011].

[6] A. T. Campbell, S. B. Eisenman, N. D. Lane *et al.*, "The Rise of People-Centric Sensing," *IEEE Internet Computing,* vol. 12, no. 4, pp. 12-21, 2008.

[7] Peter Corke, Shondip Sen, Pavan Sikka *et al.*, *Wireless Sensor and Actuator Networks,* Progress Report, Commonwealth Scientific and Industrial Research Organisation,CSIRO, 2006.

[8] G. H. Zhang, C. C. Y. Poon, and Y. T. Zhang, "A Review on Body Area Networks Security for Healthcare," *ISRN Communications and Networking*, vol. 2011, 2011.

[9] M. Chen;, S. Gonzalez;, A. Vasilakos; *et al.*, "Body Area Networks: A Survey," *ACM/Springer Mobile Networks and Applications,* vol. 16, no. 2, pp. 171-193, April, 2011.

[10] L. Sang Hyuk, L. Soobin, S. Heecheol *et al.*, "Wireless sensor network design for tactical military applications : Remote large-scale environments," in Military Communications Conference, 2009. MILCOM 2009. IEEE, 2009, pp. 1-7.

[11] S. Hussain, S. Schaffner, and D. Moseychuck, "Applications of Wireless Sensor Networks and RFID in a Smart Home Environment," in Communication Networks and Services Research Conference, 2009. CNSR '09. Seventh Annual, 2009, pp. 153-157.

[12] V. Nainwal, P. J. Pramod, and S. V. Srikanth, "Design and implementation of a remote surveillance and monitoring system using Wireless Sensor Networks," in Electronics Computer Technology (ICECT), 2011 3rd International Conference on, pp. 186-189.

[13] T. A. Dahlberg, A. Nasipuri, and T. C, "Explorerobots: A mobile network experimentation testbed," in ACM SIGCOMM workshop on experimental approaches to wireless network design and analysis, New York, 2005, pp. 76-81.

[14] S. W. Arvinderpal, "Energy Analysis of Public-Key Cryptography for Wireless Sensor Networks," in IEEE International Conference on Pervasive Computing and Communications, 2005, pp. 324-328.

[15] G. de Meulenaer, F. Gosset, F. X. Standaert *et al.*, "On the Energy Cost of Communication and Cryptography in Wireless Sensor Networks," in Networking and Communications, 2008. WIMOB '08. IEEE International Conference on Wireless and Mobile Computing, 2008, pp. 580-585.

[16] H. Lian, Z. Xuecheng, L. Zhenglin *et al.*, "An Energy-Efficient AES-CCM Implementation for IEEE802.15.4 Wireless Sensor Networks," in Networks Security, Wireless Communications and Trusted Computing, 2009. NSWCTC '09. International Conference on, 2009, pp. 394-397.

[17] L. Wei, L. Rong, and Y. Huazhong, "Cryptography Overhead Evaluation and Analysis for Wireless Sensor Networks," in Communications and Mobile Computing, 2009. CMC '09. WRI International Conference on, 2009, pp. 496-501.

[18] M. Abdalla, D. Pointcheval, P.-A. Fouque *et al.*, "An Efficient Identity-Based Online/Offline Encryption Scheme," *Applied Cryptography and Network Security,* Lecture Notes in Computer Science, pp. 156-167: Springer Berlin / Heidelberg, 2009.

[19] G. Gaubatz, J. P. Kaps, E. Ozturk *et al.*, "State of the art in ultra-low power public key cryptography for wireless sensor networks," in Pervasive Computing and Communications Workshops, 2005. PerCom 2005 Workshops. Third IEEE International Conference on, 2005, pp. 146-150.

[20] C. Karlof, N. Sastry, and D. Wagner, "TinySec: a link layer security architecture for wireless sensor networks," in Proceedings of the 2nd international conference on Embedded networked sensor systems, Baltimore, MD, USA, 2004.

[21] M. Luk, G. Mezzour, A. Perrig *et al.*, "MiniSec: A Secure Sensor Network Communication Architecture." pp. 479-488.

[22] M. Blaze, J. Feigenbaum, and J. Lacy, "Decentralized Trust Management," in Proceedings of the 1996 IEEE Symposium on Security and Privacy, 1996.

[23] J. Lopez, r. Roman, I. Agudo *et al.*, "Trust Management System for Wireless Sensor Networks: best Practices," *Computer Communications*, 2010.

[24] R. A. Shaikh, H. Jameel, L. Sungyoung *et al.*, "Trust Management Problem in Distributed Wireless Sensor Networks." pp. 411-414.

[25] T. C. Groups. "Trusted Platform Module(TPM) Summary," 8 July 2009, 2009; http://www.trustedcomputinggroup.org/resources/trusted_platform_module_tpm_summary.

[26] ARM, "ARM1176JZF-S Technical Reference Manual," http://infocenter.arm.com, [18 June, 2010].

[27] J. Azema, and G. Fayad, "M-Shield Mobile Security Technology: making the wireless secure," www.ti.com/m-shield, [Mac 2011, 2008].

[28] U. Roedig, C. Sreenan, W. Hu *et al.*, "secFleck: A Public Key Technology Platform for Wireless Sensor Networks," *Wireless Sensor Networks*, Lecture Notes in Computer Science, pp. 296-311: Springer Berlin / Heidelberg, 2009.

[29] T. Winkler, and B. Rinner, "Securing Embedded Smart Cameras with Trusted Computing," *EURASIP Journal on Wireless Communications and Networking*, vol. 2011, 2011.