Contents lists available at www.innovativejournal.in

Asian Journal of Computer Science and Information Technology

Journal homepage: http://www.innovativejournal.in/index.php/ajcsit

ISSN 2249 - 5126

# SECURITY ANALYSIS USING HANDOVER STRATEGIES FOR MULTI-HOMED BODY SENSOR NETWORKS

V. Surendra Reddy [1], **K Durga Prasad[2]***, G Sai Chaitanya Kumar [3]

*[1] Dept. of CSE, Sri Viveka College of Engg & Tech, Vijayawada, A.P.,India.*

*[2] Asst.Professor, Dept. of CSE, Sri Viveka College of Engg & Tech, Vijayawada, A.P.,India.*

*[3]Asst.Professor, Dept. of CSE, Paladugu Parvathi Devi College of Engg & Tech, Vijayawada, A.P.,India.*

## ARTICLE INFO

**Corresponding Author:**
K Durga Prasad
Asst.Professor, Department of CSE, Sri Viveka College of Engg & Tech, Vijayawada, Andhra Pradesh, India
dpkondisetty@gmail.com.

**KeyWords:** Multi-homing, Body Sensor Network, Handover, Wireless Sensor Network (WSN), Security.

## ABSTRACT

The emergence of sensor networks as one of the dominant technology trends in the coming decades has posed numerous unique challenges to researchers. These networks are likely to be composed of hundreds, and potentially thousands of tiny sensor nodes, functioning autonomously, and in many cases, without access to renewable energy resources. Cost constraints and the need for ubiquitous, invisible deployments will result in small sized, resource-constrained sensor nodes. While the set of challenges in sensor networks are diverse, we focus on security of Wireless Sensor Network in this paper. We propose some of the security goal for Wireless Sensor Network. Further, security being vital to the acceptance and use of sensor networks for many applications; we have made an in depth threat analysis of Wireless Sensor Network. We also propose some countermeasures against these threats in Wireless Sensor Network.

## INTRODUCTION

Wireless sensor networks have been developing rapidly in recent years. Much effort has been put into the exploration of wireless sensor network applications. Body sensor network for medical care is an emerging branch amongst these applications. They use wearable sensors to continuously monitor patient vital signs such as respiration, oxygen in the blood, temperature and electrocardiogram (ECG) etc. The real-time vital sign information can be delivered to doctors, nurses or other caregivers through the communication module in the wireless sensor node. Through a body sensor network, patient status monitoring can be extended from hospital to home, working place or other public locations. Any changes in patient status can be reported immediately to corresponding responders. This can expand the reach of current healthcare solutions, provide more convenience for patients and potentially increase patient survival probability in the case of emergency situations such as heart attack. Currently, many solutions for body sensor networks use a Personal Digital Assistant (PDA) on a patient to gather data from sensors and forward the data to a central server through cellular networks.

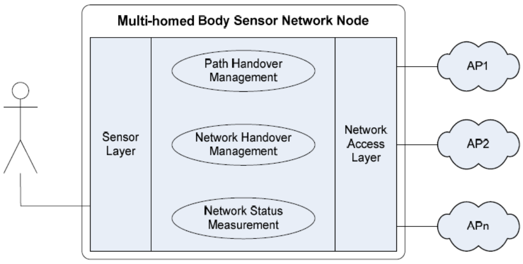
## RELATED WORK

In a remote heart monitoring system is proposed. It transmits ECG signals to a PDA which forwards the signals to the central server through the cellular network. In a wearable MIThril system is proposed. It uses a PDA to capture ECG data, GPS position, skin temperature and galvanic skin response. In a body sensor network hardware development platform is presented. It is also based on the sensor node plus PDA solution.

### *System Design*

The wearable sensor node is deployed on patient. Each node has multiple Bluetooth interfaces which are connected to ambient separate Bluetooth access points. The sensor node selects one network interface to transmit data. If the network interface fails, it switches to another interface to transmit data. The failed interface keeps searching available access points. It attaches to one of the access points except those that have been used by other interfaces.

**Figure 1: Architecture of Body Sensor Network Node**


Multi-homed Body Sensor Network Node
Path Handover Management
Sensor Layer
Network Handover Management
Network Access Layer
Network Status Measurement
AP1
AP2
APn

The architecture of the body sensor node is shown in Figure 1. The communication entity includes three modules:

- Network Status Measurement (NSM): NSM provides local and end-to-end network dimensioning information such as available access points, available bandwidth, delay, jitter, and loss to other modules in the system.

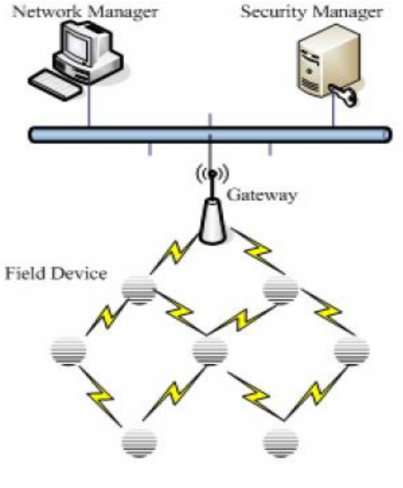
- Network Handover Management (NHM): NHM select one of the available access points which are provided by NSM.
- Path Handover Management (PHM): PHM manages end-to-end switchover amongst connections between the source sensor node and the destination central server. A connection is identified by source address and destination address. PHM makes a path handover decision based on the network status information provided by NSM.

## WSN ARCHITECTURE

In a typical WSN we see following network components –

- Sensor motes (Field devices) – Field devices are mounted in the process and must be capable of routing packets on behalf of other devices. In most cases they characterize or control the process or process equipment. A router is a special type of field device that does not have process sensor or control equipment and as such does not interface with the process itself.
- Gateway or Access points – A Gateway enables communication between Host application and field devices.
- Network manager – A Network Manager is responsible for configuration of the network, scheduling communication between devices (i.e., configuring super frames), management of the routing tables and monitoring and reporting the health of the network.
- Security manager – The Security Manager is responsible for the generation, storage, and management of keys.

**Figure 2: WSN Architecture**



## WSN SECURITY ANALYSIS

Simplicity in Wireless Sensor Network with resource constrained nodes makes them extremely vulnerable to variety of attacks. Attackers can eavesdrop on our radio transmissions, inject bits in the channel, replay previously heard packets and many more. Securing the Wireless Sensor Network needs to make the network support all security properties: confidentiality, integrity, authenticity and availability. Attackers may deploy a few malicious nodes with similar hardware capabilities as the legitimate nodes that might collude to attack the system cooperatively. The attacker may come upon these malicious nodes by purchasing them separately, or by "turning" a few legitimate nodes by capturing them and physically overwriting their memory. Also, in some cases colluding nodes might have high-quality communications links available for coordinating their attack. Sensor nodes may not be tamper resistant and if an adversary compromises a node, she can extract all key material, data, and code stored on that node. While tamper resistance might be a viable defense for physical node compromise for some networks, we do not see it as a general purpose solution. Extremely effective tamper resistance tends to add significant per-unit cost, and sensor nodes are intended to be very inexpensive.

### Sybil:

Sybil attack is defined as a "malicious device illegitimately taking on multiple identities". Using the Sybil attack, an adversary can "be in more than one place at once" as a single node presents multiple identities to other nodes in the network which can significantly reduce the effectiveness of fault tolerant schemes such as distributed storage, disparity and multipath. It may be extremely difficult for an adversary to launch such an attack in a network where every pair of neighboring nodes uses a unique key to initialize frequency hopping or spread spectrum communication. Sybil attacks also pose a significant threat to geographic routing protocols.

### Wormhole

In the wormhole attack, an adversary tunnels messages received in one part of the network over a low latency link and replays them in a different part. An adversary situated close to a base station may be able to completely disrupt routing by creating a well-placed wormhole. An adversary could convince nodes that would normally be multiple hops from a base station that they are only one or two hops away via the wormhole. This can create a sinkhole: since the adversary on the other side of the wormhole can artificially provide a high-quality route to the base station, potentially all traffic in the surrounding area will be drawn through her if alternate routes are significantly less attractive.

## COUNTER MEASURES

### The Sybil attacks

An insider cannot be prevented from participating in the network, but she should only be able to do so using the identities of the nodes she has compromised. Using a globally shared key allows an insider to masquerade as any (possibly even nonexistent) node. Identities must be verified. In the traditional setting, this might be done using public key cryptography, but generating and verifying digital signatures is beyond the capabilities of sensor nodes. One solution is to have every node share a unique symmetric key with a trusted base station. Two nodes can then use a Needham-Schroeder like protocol to verify each other's identity and establish a shared key. A pair of neighboring nodes can use the resulting key to implement an authenticated, encrypted link between them. In order to prevent an insider from wandering around a stationary network and establishing shared keys with every node in the network, the base station can reasonably limit the number of neighbors a node is allowed to have and send an error message when a node exceeds it. Thus, when a node is compromised, it is restricted to (meaningfully) communicating only with its verified neighbors. This is not to say that nodes are forbidden from sending messages to base stations or aggregation points multiple hops away, but they are restricted from using any node except their verified neighbors to do so. In addition, an adversary can still use a wormhole to create an artificial link between two nodes to convince them they are neighbors, but the adversary will not be able to eavesdrop on or modify any future communications between them.

**Wormhole and Sinkhole attacks**

Wormhole and sinkhole attacks are very difficult to defend against, especially when the two are used in combination. Wormholes are hard to detect because they use a private, out-of-band channel invisible to the underlying sensor network. Sinkholes are difficult to defend against in protocols that use advertised information such as remaining energy or an estimate of end-to-end reliability to construct a routing topology because this information is hard to verify. Routes that minimize the hop-count to a base station are easier to verify, however hop-count can be completely misrepresented through a wormhole. When routes are established simply based on the reception of a packet as in Tiny OS beaconing or directed diffusion, sinkholes are easy to create because there is no information for a defender to verify. A technique for detecting wormhole attacks is presented in, but it requires extremely tight time synchronization and is thus infeasible for most sensor networks. Because it is extremely difficult to retrofit existing protocols with defenses against these attacks, the best solution is to carefully design routing protocols in which wormholes and sinkholes are meaningless.

## CONCLUSION

Security in Wireless Sensor Network is vital to the acceptance and use of sensor networks. In particular, Wireless Sensor Network product in industry will not get acceptance unless there is a fool proof security to the network. In this paper, we have made a threat analysis to the Wireless Sensor Network and suggested some counter measures. Link layer encryption and authentication mechanisms may be a reasonable first approximation for defense against mote class outsiders, but cryptography is not enough to defend against laptop-class adversaries and insiders: careful protocol design is needed as well.

## REFERENCES

[1]. Guangzhong Yang (2006). Body Sensor Networks. Springer, ISBN: 978-1-84628-272-0.

[2]. ROSS P.E. (2004). Managing Care through the Air. IEEE Spectrum, 14-19.

[3]. PENTLAND A. (2004). Healthwear: Medical Technology Becomes Wearable. IEEE Computer, 37(5): 42-49.

[4]. B Lo, S Thiemjarus, R King, G Yang (2005). BODY SENSOR NETWORK – A WIRELESS SENSOR PLATFORM FOR PERVASIVE HEALTHCARE MONITORING. The 3rd International Conference on Pervasive Computing.

[5]. Y. Zou, K. Chakrabarty, "Sensor deployment and target localization based on virtual forces", INFOCOM 2003. Twenty- Second Annual Joint Conference of the IEEE Computer and Communications Societies. IEEE, Volume: 2, Pages: 1293 - 1303, April 2003.

[6]. IEEE 802.15.1 (2005). Wireless medium access control (MAC) and physical layer (PHY) specifications for wireless personal area networks (WPANs).

[7]. J. R. Douceur, "The Sybil Attack," in 1st International Workshop on Peer-to-Peer Systems (IPTPS '02), March 2002.

[8]. Castro and Liskov, "Practical byzantine fault tolerance," in OSDI: Symposium on Operating Systems Design and Implementation. USENIX Association, Co-sponsored by IEEE TCOS and ACM SIGOPS, 1999.

[9]. A. Banerjea, "A taxonomy of dispersity routing schemes for fault tolerant real-time channels," in Proceedings of ECMAST, vol. 26, May 1996, pp.129-148.