ISSN:1991-8178

**Australian Journal of Basic and Applied Sciences**

Journal home page: www.ajbasweb.com

# HBSIDS: Improving Energy Efficiency of Human Body Sensor Based Intrusion Detection System in a Cooperative Network

[1]Gopal R and [2]Parthasarathy V

*[1]Chettinad college of Engineering & Technology, Department of Computer Science and Engineering, Karur, Tamil Nadu, India*
*[2]Vel Tech Multi Tech Dr.RR Dr.SR Engineering College, Department of Computer Science & Engineering, Avadi, Chennai, Tamil Nadu, India.*

**ARTICLE INFO**

***Article history:***
*Received 6 March 2015*
*Accepted 25 May 2015*
*Published 29 June 2015*

***Keywords:***
*Cooperative Network, Human Body Sensor, Intrusion Detection System.*

**ABSTRACT**

**Background:** Nowadays Cooperative Network is drastically growing and applied in various applications such as Military, Hospital, and Police, etc. In this paper Military application is taken as an example, analyzed the functionality of the cooperative network. Human wearable sensor devices are used to monitor the human motion within a Military Region. In this paper, it is aimed to monitor and detect intruders [contradictory action / behavior] among entire soldiers in a Military-Network using HBSIDS-[Human Body Sensor based Intrusion Detection System]. Since soldiers are considered as nodes in a cooperative network, each node is integrated with wearable sensor nodes in their body. The wearable sensor devices are well configured should cooperate to each other within the region and also with the Base station. If any node moves in the wrong direction, communicate with other unknown nodes, dropping wrong information or communicate with wrong messages those nodes are detected as malicious nodes and eliminated from the network by monitoring wearable sensors. To avoid this situation a key management method, KIDHBS is proposed for communication following Identity Based Encryption technique available already in the literature. During the Monitoring process, it is essential to check the energy of the wearable sensor device to avoid the low battery based data loss integrated with RTS/CTS mechanism. HBSIDS is simulated in NS2 software and the results show that HBSIDS can provide better performance than the existing approaches.



**To Cite This Article:** Gopal R and Parthasarathy V., HBSIDS: Improving Energy Efficiency of Human Body Sensor Based Intrusion Detection System in a Cooperative Network. ***Aust. J. Basic & Appl. Sci.,*** *9(20): 551-558, 2015*

## INTRODUCTION

Today WSN extends its features where one of the features is node co-operation. Nodes in cooperative network can transmit data only, if the channel is good, nodes are honesty and verify nodes as good node or malicious node. Various constrain [distance, frequency, communication mechanism and individuality] based people, regularly connected to the connectors, assume a vital part in data dispersion (Gladwell, 2000). Replies to these inquiries have been utilized to comprehend the achievement and adequacy of a work bunch or an association all in all. In the earlier researches coopMAC, slot allocation, RTS/CTS and various schemes are proposed to provide complete security in terms of node authenticity, data integrity and so on.

In (Wei and Ming , 2014, Shnayder, Chen, Lorincz, Thaddeus, Fulford., and Welsh., 2005) the author considered about the PSDBS-[Publisher Subscriber Driven Body Sensor] networks, where a dynamic key is enabled for the design and development of CBS[Code Blue System]. In this paper, it is considered that the communication happen among the human body sensor based cooperative networks. The human network is well defined and configured with the body sensor devices and each sensor device is assigned by a key for verifying the originality of the sensor devices. In this method, integrity, confidentiality, authenticity of the safe data transmission in the network is preserved.

### *Literature Survey:*

Various procedures have been developed and proposed to catch or anticipate malevolent action in wireless networks. Given below are the summaries of a small amount of papers discussed already: In (Kejun, Jing, Varshney and Balakrishnan, 2006 and Chobe and Deepali, 2013), the author proposed the 2ACK system that supports as an extra method for directing network protocol to sense routing rowdiness and to reduce their denying behavior. The key impression of the 2ACK system is that it will send 2 hop reply packets. Routing overhead is

**Corresponding Author:** Gopal R, Chettinad college of Engineering & Technology, Department of Computer Science and Engineering, Karur, Tamil Nadu, India.
+91 9791410125, E-mail: rgopalkarur@gmail.com.

reduced in 2ACK system. The thought of nuggets is utilized as an installment is discussed in (Jakobsson, and Nodeaux, and Butty, 2003). There are two prototypes1) Packet exchange sort 2) Packet backpack sort. In the Packet Trade sort, intermediate nodes buy the packet from its sender for few nugglets and sell it to receiver node for more nugglets (Jakobsson, and Nodeaux, and Butty, 2003).

In (Marti, and Giuli, and Lai, and Baker, 2000), the watchdog and the path rater component are utilized to distinguish and dispose of the malicious nodes. In (Yuan xue, and Klara, 2004), it additionally utilizes end-to-end ACKs. In (Khatawkar, Kulkarni, and Pandyaji, 2011), different protocols and techniques were examined that deliver an extra method to identify bad routing behavior and to alleviate their unfavorable character. Yet applying checking instrument to accept every individual node in the network brings more impact than different systems. (Manjula, and Chellappan, 2012) Proposes a procedure called randomized and Trust based watcher judgment technique for duplication attack identification systems in wireless networks (RTRADP) utilizing the trust element. In (Camilo, Carreto, Silva, and Boavida, 2006), network life time can be increased by using an Energy Efficient Ant Based routing algorithm. It is necessary to increase the network lifetime in terms of sensors, energy where it makes the data loss during the data transmission. In this paper, it is aimed to provide an IDS via human body wearable sensor devices with having highest energy.

***Existing System:***

Intruder node can be controlled and differentiated using IDS (Hatware, Kathole and Bompilwar, 2012), cooperative IDS, and Watchdog-path rater techniques and so on. In ad-hoc networks the identity verification of each node is important to distinguish security attacks in the network. Malicious nodes may be of two types, for example, childish and vindictive nodes are looking into.

Our contribution of the paper is:

- Intrusion Detection through human body wearable sensor devices.
- Verify the energy value of the sensor device before communication.
- Define a lifetime of the sensor device and recharge the battery within the stipulated time.

***Proposed System:***

It is considered that a network region **RG = {N1, N2, N3… Nm}**. Where each **Ni** is a collection of sensor nodes have integrated with body sensors. Each node is defined with an initial energy **EI**. These nodes are able to sense and deliver some of the properties needed for detecting intrusion, which are Spatio-Temporal properties, Behavioral properties and physiological properties. The sub property values [Taxonomy] of the above properties are shown in detail in Fig.1. For each activity, the sensor node needs some energy. Some of the energy is reduced from the initialized energy for each activity. The human sensor nodes are well trained nodes assigned with predefined functionalities like turn, walk, run, speak, and fire [shoot] and so on. It is assumed that the human sensor nodes cannot do their own jobs within the region. The nodes should follow the commander node command and do a task. The property values indicate the static and dynamic behavior of each node within the region. From these values, it is very easy and fast to decide about a node behavior. From the node behavior, it can be concluded that the node is an honest node or a malicious node. There are three types of properties can be verified on a node to provide tight security in the network. Those properties can be verified with the key verification for a sensor node can improve the efficiency of the security application in a human network.

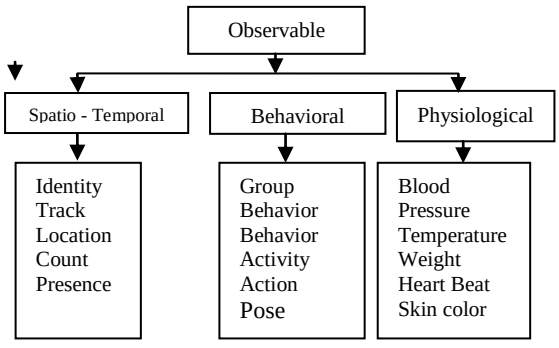



**Fig. 1:** It is clear that the node's personal properties, dynamic properties and health properties are sensed while communication and node activation.

The network G split into various sized regions; nodes are randomly or uniformly placed in the region, according to the nature of the network behavior. Each node in the region is attached to sensors in their body from neck to leg shown in Fig.2a clearly. Each sensor is sensing quality verified

by the network administrators and it has its own lifetime. Once a node loses its energy below a threshold value, the battery is changed immediately by the main administrator and the energy becomes full.

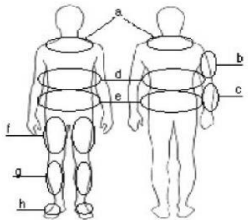



**Fig. 2a:** Position of Sensors in human body

**Fig. 2b:** Entire Nodes in a Network

Fig.2b shows the sensor nodes in the network and Fig.2c shows an amount of nodes are selected and placed in a region in a uniform manner for a specific task. Each node can communicate together as well as to the base station with cooperation. Also, it is assumed that these nodes are moving around the region and do their assigned work in the network.

The human node can be placed is such a manner in order to avoid the data loss, improve the accuracy in packet delivery ratio, and reduce the energy consumption. A small portion of the human node placement is shown in Figure-2c. From this Fig.2c, it is clear that the distance among the nodes is uniform, direction focused; communication method is many-to-many communication. Where the many-to-many communication is restricted by RTS-CTS and scheduling method described below.

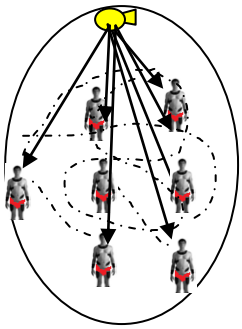
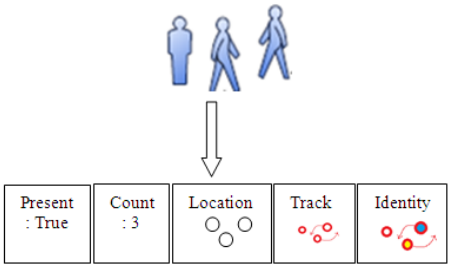


**Fig. 2c:** Elected Nodes Arranged in a Region

The movement, sound, directions, positions, location and nodes physical properties are limited and restricted. When a node is elected for the network and assigned into a region based on their behavior, skill, nature of the job, their ID and own static behaviors and are recorded and fed into sensor, attached into node body. It is important and unique nature that the node ID is nothing but the DNA pattern of the human node. Whenever the node passing a data to BS or monitored by a monitoring node, the complete details about the node will be watched and verified. If any ID or node information is mismatched with the recorded data of that particular node, it is treated as intruder node and eliminated from the network.




Whenever a node deployed into the region, the node status is updated.

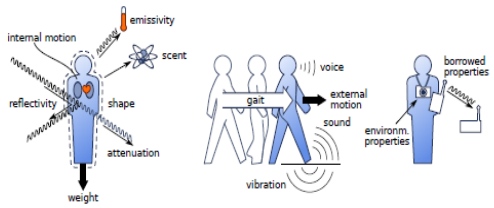
Means:

$$Node - Present = True;$$

$$Node - count = i \; \forall \, i \; varies \; from \; 1 \; to \; m$$

***Node-EI = 100;***

Where **m** is the total number of nodes deployed in the region. The monitoring node [Sensor or sensor Camera ] monitors or sense the information about the nodes in the region and transmit to the BS for verification. The various kinds of proprties are sensed from the sesor nodes from the human body is depicted in Fig.4




Static Properties Dynamic Properties External Properties

**Fig. 4:** Properties of Human Body Sensors

***Hbsids:***

It is assumed that the authorized human node can have a communication with the other nodes in the network. Our proposed approach consists of two main parts for secured communication. One is the DNA pattern and the other is key based verification. Also the MAC based communication can help the

The MAC protocol used in MANETs is the IEEE 802.11 DCF (CSMA/CA with RTS/CTS) mechanism. In 802.11, collisions between nodes are avoid by carrier sensing before transmission. Node will deter its transmission if the channel is busy and enters into backoff mode.If the channel sensed is free then the node enters into dialog mode and then transmit the packets.

The number of collisions can be reduced by using CSMA/CA. RTS/CTS will reserves the channel spatially and temporarily. Hidden terminal problem is avoided by RTS/CTS. But it in turn reduce the bandwidth usage in the network.

Collisions may also happen and may degrade performance in some cases. When the density of the network is high, then number of collision will get increased.In order to avoid this, the clear to send must be transmitted a number of times. But in this network, the overhead caused due to the CTS multi transmission will outweighted the gain.

In the power consuming mechanism, data packet and ACK packets are forwarded witht the minimum power needed to reachout the destination or the source node respectively. RTS/CTS packets are transmitted with a max power level. Collision must be avoided because it will introduce retransmission of the data packets or ACK which in turn will consume additional power.

HBSIDS detects an intruder node within entire nodes in the region using the sensed human sensor properties. These properties indicates the static values which defines the sensor node characteristics like height, weight, shape, internal activity of the node with the ID [DNA-pattern]. The node informations are verified according the data transmission format given below

| ID | Place | Direction | Poistion | Height | |
|---|---|---|---|---|---|
| | Weight | Heart beat | Body heat | ….. | Count |

**Fig. 5:** Packet Fromat

In the region **R**, if a node **A** is a good node then the ID [DNA-pattern] is correct with the other static and dynamic values of the node. There are three ways a node can be treated as malicious node.

- One, if node B is a malicious node, it uses the other nodes' sensor device, and it will be detected when the sensor device broadcast the ID correctly by the other information is wrong.

- Two, if the dynamic behavior like turn, walk and run [should reflect in internal body properties ECG, EEG] are mismatched with standard value, that node is treated as malicious node.
- Finally, if the node borrowed properties [sending and receiving data] are not from the administrator or from the BS then the node is treated as malicious node.

***Energy Computation:***

The network lifetime of WSN is defined commonly by the time span from start of the node operations to the first dead node (Mehdi, Yousef, and Saman Siavoshi, 2014). But in this paper, the application is military based and considering the human body sensors, the life of the sensor is defined by the time span from the start of the node deployment to the dead state of that particular node. In this HSIDS based cooperative sensor network, if any one of the node dead, then the cooperation among the nodes cannot be carried out.

It is considered that the energy of each node depends only it network operations. Also the energy of the sensor node cannot be balanced with other nodes in the route or in the network. However, the nodes within a predefined region are closer to each one, the senor energy consumption is very less for each activity and life time is more. In the military applications, the required communication is more and need more energy. Thus, we consider the lifetime of the region and sensor is considered as a square M x M area and its distance from the nodes to BS is U.

In this section, it is presented that the design of node communication follows the adhoc routing protocol and it has some phases like route discovery and data transmission. In our approach the communication is one-to-one or one-to-many. During the route discovery and data transmission, RTS-CTS method is followed from AASR protocol (Wei Liu, and Ming Yu, 2014) for reducing the message overhead, packet overhead and discovering a secured route. Also, this RTS-CTS method can provide protection for anonymous packet exchange during routing. It also saves the energy consumption. Next, the packet scheduling method is applied for energy consumption. The scheduling first divide the available bandwidth among the various service levels to provide high priority and the remaining bandwidth can be used for number of ways. In our approach, all the nodes in the network should follows the same scheduling method while data transmission in order to save the energy.

***Simulation And Results:***

The overall functionality of the HBSIDS system is coded and simulated in Network Simulator-2 software and the performance is verified. The relevant parameters assigned in Network Simulator are given in Table-2.

**Table 2:** Simulation Settings

| | |
|---|---|
| Area | 1200 x 1200 |
| Nodes | 10, 20, 30, 40, 50, 100 |
| Packet Size | 50 |
| Transmission Protocol | AODV |
| Application Traffic | CBR –TCP - UDP |
| Simulation Time | 50 ms |
| Queue Type | Drop-Tail |
| Propagation Model | Two Ray Ground |
| Antenna Model | Omni Antenna |
| Routing Protocol | AODV |
| Initial Energy | 100 J |

The metrics analyzed for verifying the HBSIDS performance are throughput, energy, delay and number of attacker detected. For computing the performance metrics the number of nodes deployed in various rounds are changed like 25, 50, 75 and 100 and computed. The percentage of throughput obtained and percentage remaining energy in the network and percentage of delay taken by HBSIDS is shown in Fig.6, 7, 8 and Fig.9.

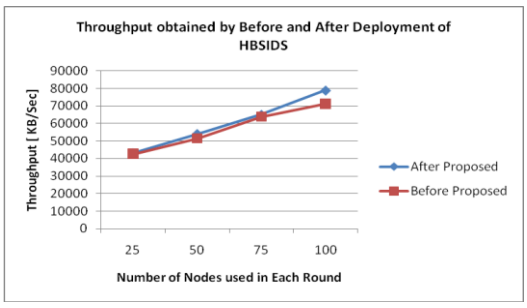



**Fig. 6:** Throughput obtained by proposed system vs. Existing System

As far as throughput the HBSIDS acquired more fruitful transmission than the current methodology and it plainly portrayed in Fig.6. The HBSIDS transmitted 43000, 54000, 65000 and 78900 packets in all the four rounds with 25, 50, 75 and 100 nodes separately where the existing framework transmitted 42500, 51345, 63749 and 71234 packets in all the four rounds with 25, 50, 75 and 100 nodes individually.

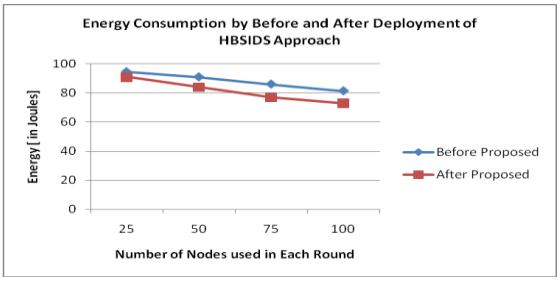



**Fig. 7:** Energy Consumption by Proposed approach vs. Existing approach

If there should be an occurrence of energy sparing the HBSIDS holds more energy than existing methodology and it obviously delineated in Fig.7. The proposed methodology holds 94.58%, 91%, 86% and 81.34% of the energy in all the four rounds with 20, 40, 60, 80 and 100 nodes separately where the existing system holds 91%, 84%, 77% and 73% of the energy in all the four rounds with 20, 40, 60, 80 and 100 nodes individually.

Delay is computed as the time duration taken between sending time and receiving time among source node, destination node. HBSIDS takes less delay for all the simulation round done. As the number of node increases, the delay increases gradually in both existing system and proposed system. The delay taken by the proposed approach is very less than the existing approach and it is shown in Fig.7.

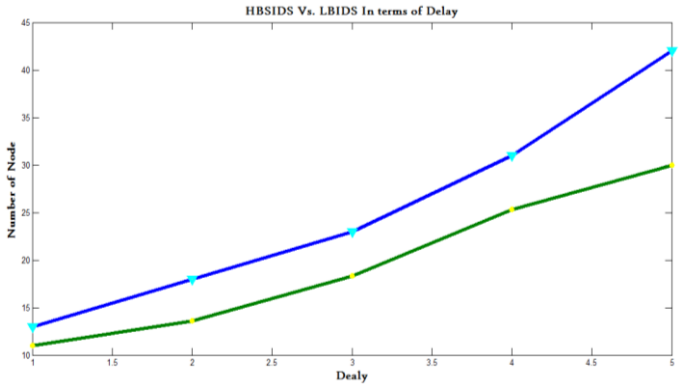



**Fig. 7:** Delay Comparison by HBSIDS vs. LBIDS

A malicious node can be detected by the ID-[DNA] with other relevant information assigned during node birth. In this paper there certain number of malicious node is increasing rabidly due to the number of node increased in the network in LBIDS. But in HBSIDS, the number of malicious node activity is more or less completely controlled and detecting less number of malicious nodes and is shown in Fig.8.

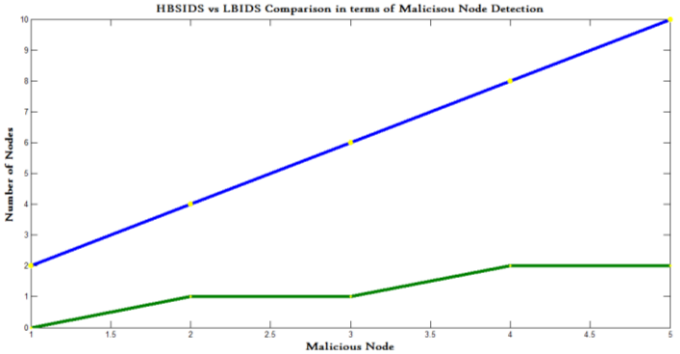



**Fig. 8:** Malicious Node Detection Comparison by HBSIDS vs. LBIDS

One of the main objectives of this paper is to improve the energy efficiency also. To reduce the energy consumption, RTS-CTS based communication, scheduling based data transmission. To evaluate the performance of the proposed approach, there are five rounds of data transmission operations are applied on various numbers of nodes deployed in the network. The number of nodes deployed is 20, 40, 60, 80 and 100. In end of each round, the remaining energy is computed and the performance is analyzed. In our approach the communication is very less and the range of communication is also less. Since, the performance obtained from the simulation is shown in the following Fig.9.

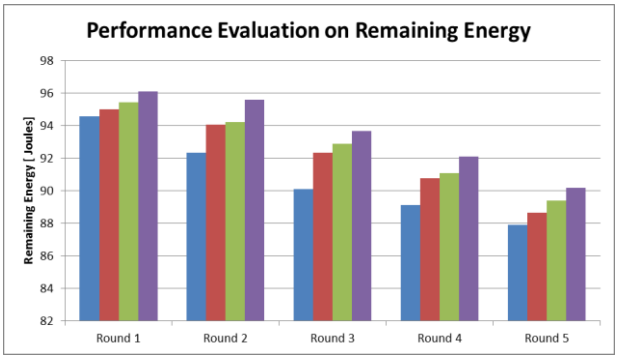



**Fig. 9:** Performance Evaluation on Energy Consumption

***Conclusion:***

In this paper HBSIDS verifies each node in all the levels of communication whether the node as normal node or malicious node. The unique advantage of this paper is the human body sensor nodes are more accurate in detecting malicious nodes than other sensor nodes. The internal properties, static properties and dynamic properties are reflecting the behavior of the human sensor node where it can verify the node activity. HBSIDS approach compares and verifies the node behavior by utilizing all the three kinds of properties without affecting the quality of service metrics in the network. Also the DNA pattern based Node-ID provides more accuracy in Node-ID verification.

In future work the size of the network region can be increased and also the nodes in this region can be increased and the performance of HBSIDS can be measured.

## REFERENCES

Gladwell, M., 2000. The Tipping Point: How little things make can make a big difference. New York: Little Brown.

Isha V. Hatware., Atul B. Kathole., Mahesh D. Bompilwar, 2012. Detection of Misbehaving Nodes in Ad Hoc Routing. IJETAE, ISSN 2250-2459, 2: 2.

Kejun Liu., Jing Deng., Pramod K. Varshney and Kashyap Balakrishnan, 2006. An Acknowledgment - based Approach for the Detection of Routing Misbehavior in MANETs. http://www.uncg.edu/cmp/faculty/j_deng/.

Chobe., S.N., Deepali Gothawal., 2013. An Acknowledgement Based Approach For Routing Misbehavior Detection In MANET With AOMDV. Proceedings of International Joint Conference, Goa, India, ISBN: 978-81-927147-7-6.

Jakobsson, M and J.P. Nodeaux and Butty., 2003. A micro-payment scheme encouraging collaboration in multi-hop cellular networks. Computer Aided Verification, Springer, pp: 15-33.

Marti, S. and T.J. Giuli and K. Lai and M. Baker, 2000. Mitigating routing misbehavior in mobile ad hoc networks. ICOMCAN: volume=6:255-265.

Yuan xue., and Klara Nahrstedt., 2004.Providing Fault-Tolerant Ad hoc Routing Service in Adversarial Environments. Wireless Personal communications, 29: 367.

Khatawkar., S.D., U.L. Kulkarni and K.K. Pandyaji, 2011. Detection of Routing Misbehavior in MANETs. IACSIT Press, Singapore.

Manjula., V. and C. Chellappan, 2012. Trust Based Node Replication Attack Detection Protocol for Wireless Sensor Networks. Journal of Computer Science, 8: 1880-1888.

Camilo., T., C. Carreto, J. S´a Silva and F. Boavida, 2006. An energy-efficient ant base routing algorithm for wireless sensor networks. Proceedings of the 5th International Workshop on Ant Colony Optimization and Swarm Intelligence (ANTS '06), 49-59.

Pathan., A.S.K and C.S. Hong, 2008. SERP: Secure energy-efficient routing protocol for densely deployed wireless sensor networks. Annales des Telecommunications/Annals of Telecommunications, 63: 529-541.

Mehdi Tarhani., Yousef S. Kavian and Saman Siavoshi, 2014. SEECH: Scalable Energy Efficient Clustering Hierarchy Protocol in Wireless Sensor Networks. IEEE SENSORS JOURNAL, 14:11.

Wei Liu., and Ming Yu., 2014. AASR: Authenticated Anonymous Secure Routing for MANETs in Adversarial Environments. IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY.

Shnayder., V., B. Chen, K. Lorincz, R.F. Thaddeus, J. Fulford and M. Welsh, 2005. Sensor Networks for Medical Care. Technical Report TR-08-05, Division of Engineering and Applied Sciences, Harvard University.

Malan., D., T. Fulford-Jones, M. Welsh and S. Moulton, 2004. Codeblue: An Ad hoc Sensor Network Infrastructure for Emergency Medical Care. *Proceedings of MobiSys 2004 Workshop on Applications of Mobile Embedded Systems* (WAMES 2004).