Lightweight Trust Management of Wireless Medical Sensor Network

K.T.MeenaAbarna[1], Dr.K.Venkatachalapathy[2],

[1]*Assistant Professor, Dept. of Computer Science Engineering, Annamalai University, Annamalai Nagar-608 002.*

[2]*Associate Professor, Dept. of Computer Science Engineering, Annamalai University, Annamalai Nagar-608 002.*

Abstract

Wireless medical sensor networks (WMSNs) enable ubiquitous health monitoring of users during their everyday lives, at health sites, without restricting their freedom. This issue is often ignored in existing trust systems. We identify the security and performance challenges facing a sensor network for wireless medical monitoring and suggest it should follow a two-tier architecture. Based on such architecture, we develop an attack-resistant and lightweight trust management scheme named *ReTrust*. This paper also reports the experimental results of the Collection Tree Protocol using our proposed system in a network of which show that ReTrust not only can efficiently detect malicious/faulty behaviours, but can also significantly improve the network performance in practice.

Keywords— *Terms*—Medical Sensor Networks (MSNs), network performance, security, trust management.

I. INTRODUCTION

A. WIRELESS MEDICAL SENSOR NETWORKS:

A Medical wireless sensor network (WMSN) consists of spatially distributed autonomous sensors to cooperatively monitor physical or environmental conditions, such as temperature, sound, vibration, pressure, motion or pollutants. The development of wireless sensor networks was motivated by military applications such as battlefield surveillance. They are now used in many industrial and civilian application areas, including industrial process monitoring and control, machine health monitoring, environment and habitat monitoring, healthcare applications, home automation, and traffic control.

In addition to one or more sensors, each node in a sensor network is typically equipped with a radio transceiver or other wireless communications device, a small microcontroller, and an energy source, usually a battery. A sensor node might vary in size from that of a shoebox down to the size of a grain of dust, although functioning "motes" of genuine microscopic dimensions have yet to be created. The cost of sensor nodes is similarly variable, ranging from hundreds of dollars to a few pennies, depending on the size of the sensor network and the complexity required of individual sensor nodes. Size and cost constraints on sensor nodes result in corresponding constraints on resources such as energy, memory, computational speed and bandwidth. A sensor

Network normally constitutes a wireless ad-hoc network, meaning that each sensor supports a multi-hop routing algorithm.

B.Wireless Sensor Network:

A Wireless Sensor Network (WSN) provides a low-cost and multifunctional means to link communications and computer networks to the physical world. It consists of base stations and a number of wireless sensors. Each sensor is a unit with wireless networking capability that can collect and process data independently. Sensors are used to monitor activities of objects in a specific field and transmit the information to the base station.

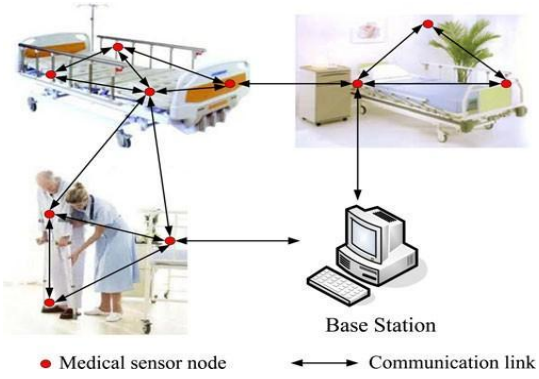


Fig. 1.Schematic diagram of an WSN.[1]

C. Overview of MSNs:

An MSN accommodates tens or hundreds of users' body sensor networks (BSNs) other SNs (e.g., sensing the temperature of a specific room) and relay nodes. Each BSN mainly consists of tiny wireless

SNs that is placed in, on, or around a patient's body. These sensors consistently monitor patients 'physiological activities and actions, such as health status and motion pattern. The sensed data from all BSNs may be sent tone local server for data processing, aggregation, or permanent records. Wireless sensors could replace existing wired telemetry systems for many specific medical applications, such as long-term ambulatory monitoring. Fig. 1 depicts an exemplary hospital MSN [1] the emergence of low-power, single- chip radios based on the Bluetooth and 802.15.4 standards has precipitated the design of small-networked medical sensors.

II. EXISTING SYSTEM

A very simple yet extremely efficient hidden-node avoidance mechanism for WSNs. H-NAM relies on a grouping strategy that splits each cluster of a WSN into disjoint groups of non-hidden nodes that scales to multiple clusters via a cluster grouping strategy that guarantees no interference between overlapping clusters Hidden-node collisions affect four QoS metrics.

1) *Throughput*, which denotes the amount of traffic successfully received by a destination node and that decreases due to additional blind collisions.
2) *Transfer delay*, which represents the time duration from the generation of a message until its correct reception by the destination node, and increases due to message retransmissions due to collisions.
3) *Energy-efficiency* that decreases since each collision causes a new retransmission.
4) *Reliability*, since applications may abort message transmission after a number of retransmissions.

A. The H-Name Mechanism:

A multiple cluster wireless network where in each cluster there is at least one node with bidirectional radio connectivity with all the other cluster nodes is considered. This node is denoted as cluster-head (CH). At least the CH must support routing capabilities, for guaranteeing total interconnectivity between cluster nodes. Nodes are assumed to contend for medium access during a contention access period (CAP), using a contention-based MAC (e.g., CSMA family). A synchronization service must exist to assure synchronization services

B. Intracluster Grouping:

Initially, all nodes in each cluster share the same CAP thus are prone to hidden-node collisions. The H-Name mechanism subdivides each cluster into node groups where all nodes have bidirectional connectivity and assigns a different time window to each group, during the CAP. The set of time windows assigned to node groups' transmissions is defined as group access period (GAP), and must be smaller or equal to the CAP. In this way, nodes belonging to groups can transmit without the risk of causing hidden-node collisions. No interference with adjacent clusters, since that might also instigate hidden-node collisions.

Step 1—Group Join Request: Let us consider a node that wants to avoid hidden-node collisions. Node sends a *Group join. Request* message to its CH, using a specific broadcast address referred to as *group management address* in the destination address field is defined as an *intracluster broadcast address*, which must be acknowledged by the CH in contrast to the typical broadcast address. Obviously, the acknowledgment message (ACK) will be received by all cluster nodes, since the CH is assumed to have bidirectional links with all of them the *Group-join. Request* message is sent using the group management address , CH sends back an ACK frame to notifying it of the correct reception of the group join request all cluster nodes in the transmission range of (thus received the *Group-join. Request* message) and that already belong to a group, check if they have already registered as a neighbour node in their *Neighbour Table*.

Met your manuscript electronically for review.

III. PROPOSED SYSTEM

To identify the security and performance challenges

Facing a sensor network for wireless medical monitoring. Two-tier architecture for an MSN. Based on the proposed two-tier architecture we develop an attack -resistant and weight trust management protocol named ReTrust which remedies the security and efficiency weaknesses of existing trust systems.

ReTrust is lightweight, since it does not impose any additional overhead on the resource poor SNs and the trust calculation on master nodes (MNs) is simple. To the best of our knowledge, this is the first attack resistant trust management protocol for

MSNs. The Collection Tree Protocol (CTP) using Tree and ReTrust, respectively, in a network of Telosb motes. ReTrust not only effectively identifies malicious behaviours and excludes malicious/faulty nodes; the security and performance challenges facing a sensor network for wireless medical monitoring and suggest it should follow two-tier architecture. Based on such an architecture, we develop an attack- resistant and lightweight trust management scheme named ReTrust A trust value is considered to be an integer in [0, λ], where 0 denotes the most untrusted state, while λ denotes the most trusted state a node's historical trust values should be taken into account in order to measure its current trustworthiness. After a unit of time elapses, the window slides one time unit forward, thereby dropping the interactions done during the first unit node x broadcasts a recommendation request message to its neighbours and waits for replies. Node x sets the hop number h of the recommendation request message propagation and then adds h to the request message. Upon receiving a request message, the neighbours will reply if they have information needed by node x.Indirect trust is established through trust propagation. Many trust models have been proposed to determine how to calculate indirect trust between two nodes from trust propagation paths. To prevent badmouthing attack, a necessary condition to trust propagation is added into the indirect trust calculation. That is, trust can propagate along path x –y–z if the recommendation trust between node x and y is greater than a threshold. In a general multihop recommendation path, this condition is held in each intermediate node.

Latency: this requirement is dictated by the applications, and may be traded for improved security and energy consumption. Replacement of batteries in MSNs nodes is much easier done than that in WSNs whose nodes can be physically unreachable after deployment. To maximize battery life time in a WSN at the expense of higher latency.

Flexibility: non-invasive sensors can be used to automatically monitor physiological readings, which can be forwarded to nearby devices (e.g., a PDA or mobile phone) according to application requirements.

Effectiveness and efficiency: the signals that body sensors collect can be effectively processed to obtain reliable and accurate physiological estimations.

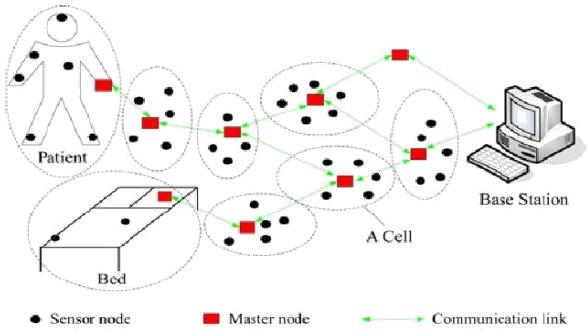


Fig 3: Two-tier Architecture

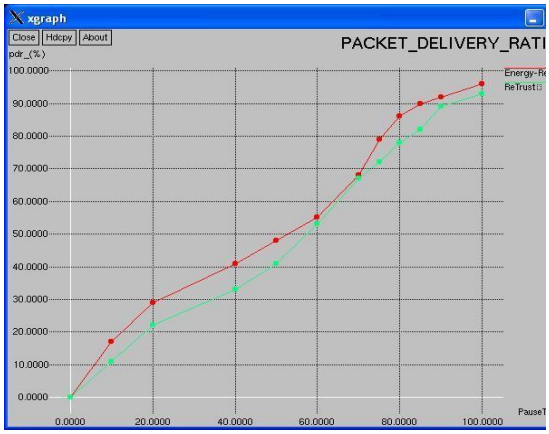
IV. IMPLEMENTATION

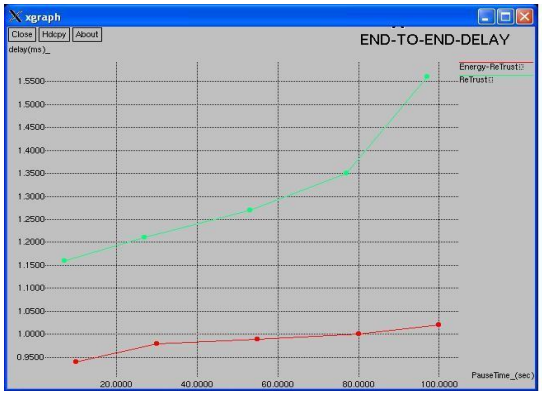
A.Trust Management in the Intracell Level

Each cell member SN is within the transmission range of the MN in ReTrust, only direct information from observation of behaviours of each SN is employed to calculate its trust value. There are many possible actions SNs would carry out in a cell of MSNs depending on different applications. The features of an MSN data processing are introduced into the trust management. The detailed description is given as follows. The quality of the data (e.g., temperature and light) reported by an SN can be used to represent the node's behaviour in data processing task.

B.Trust Management in the Inter cell Level

An each MN manages the direct trust records of its one-hop neighbouring MNs through observing their behaviours. Each MN manages the recommendation and indirect trust records of its non-one-hop neighbouring MNs. each MN submits all these records to the BS. Upon receiving this information the BS can run some efficient centralized mechanism to detect the malicious MNs. either SI (MKS) or CGS as primary units. (SI units are strongly encouraged.) English units may be used as secondary units (in parentheses).





V. Conclusion

With the emergence of widespread use of MSNs the need of a proper trust management protocol is strongly felt. An attack-resistant and lightweight trust management scheme named ReTrust for MSNs has been proposed. The security the ReTrust is feasible for enhancing the security and network performance of real MSN applications.

References

[1] Daojing He, Chun Chen, Sammy Chan, Jiajun Bu, and AthanasiosVasilakosReTrust: Attack-Resistant and Lightweight Trust Management for Medical Sensor Networks" releasevol. 16, no. 4, July 2012.

[2] O. G. Morchon and H. Baldus, "Efficient distributed security for wireless medical sensor networks," in Proc. Intell. Sensors, Sensor Netw. Inf. Process. 2008, pp., 249–254.

[3] T. Grandison and M. Sloman, "A survey of trust in internet applications," IEEE Commun. Surveys Tuts., vol. 3, no. 4, pp. 2–16, Fourth Quarter 2000.

[4] D. Ingram, "An evidence based architecture for efficient, attack-resistant computational trust dissemination in peer-to-peer networks," in Proc. iTrust 2005, pp., 273–288.

[5] [5] G. Theodorakopoulos and J. S. Baras, "Trust evaluation in ad-hoc networks,"inProc. ACM Conf. Wireless Netw. Security 2005, pp. 1–10.

[6] R. Venkataraman,M. Pushpalatha, and T. Rao, "A generalized trust framework for mobile ad hoc networks," in Recent Trends in Networks and Communications, vol. 90, N. Meghanathan, S. Boumerdassi, N. Chaki, D. Nagamalai, Eds. Berlin/Heidelberg, Germany: Springer-Verlag, 2010, pp. 326–335.

[7] K. Wang, M. Wu, and S. Shen, "A trust evaluation method for node cooperation in mobile ad hoc networks," in Proc. Int. Conf. Inf. Technol. 2008, pp., 1000–1005.

[8] [8] S. Ganeriwal, L. K. Balzano, and M. B. Srivastava, "Reputation-based framework for high integrity sensor networks," ACMTrans. Sensor Netw., vol. 4, no. 3, pp. 1–37, 2008.

[9] A. Boukerch, L. Xu, and K. EL-Khatib, "Trust-based security for wireless ad hoc and sensor networks," Comput.Commun., vol. 30, no. 11–12, pp. 2413–2427, 2007.

[10] Y. Stelios, N. Papayanoulas, P. Trakadas, S. Maniatis, H. Leligou and T. Zahariadis, "A distributed energy-aware trust management system for secure routing in wireless sensor networks," in Mobile Lightweight Wireless Systems, vol. 13, F. Granelli, C. Skianis, Y. Xiao, and S. Redana, Eds. Berlin, Germany: Springer-Verlag, 2009, pp. 85–92.

First Author

K.T.Meena Abarna received her Bachelor's degree in Computer Science & Engineering from Annamalai University, Tamilnadu, India in 2006 and her Master's degree in Computer Science & Engineering from Annamalai University, Tamilnadu, India in 2008. She is currently working as an Assistant Professor in the Department of Computer Science & Engineering, Faculty of Engineering & Technology, Annamalai University. She is having 5 years and 7 Months experience in teaching. She has published 3 research papers in International and National conferences and 1 international journal . Her field of interest includes Computer networks and Image processing. She is a life member in CSI. .

Second Author

Dr. K.Venkatachal**a**pathy received his B.Sc. degree in Physics from Madras University, Tamilnadu in 1987 and he received his Master's degree in Computer Applications from Pondicherry University in 1990. He completed his Ph.D in Computer Science & Engineering from Annamalai University, Tamilnadu, India in 2008. He is currently working as an Associate Professor in the Department of Computer Science & Engineering, Faculty of Engineering & Technology, Annamalai University. He is having 18 years of experience in teaching. He has published more than 20 research papers in international conferences and journals. His field of interest includes Image Processing and Computer networks. He is currently guiding 6 research scholars towards Ph.D. He is a life member in various professional bodies like ISTE, CSI. Etc.,