A TRUST BASED FRAMEWORK FOR SECURE DATA TRANSMISSION IN BODY AREA NETWORKS

Y.Mohideen faril sumaiya [1],

PG Student, Department Of Electronics And Communication Engineering,

Bharathiyar Institute Of Engineering For Women,

E-mail:sumaiyapersonal@gmail.com

Mrs. R. Nithyalakshmi[2],

Assistant Professor, Department Of Electronics And Communication Engineering,

Bharathiyar Institute Of Engineering For Women,

Abstract:

Body area networks (BAN) has recently emerged as an important enabling technology to support various telehealth applications. Because of its exceptional application domain, it is critical to ensure the secure and reliable gathering of patient's physiological signs. However, most of the existing security solutions for BANs focus on using encryption techniques to secure the data transmission or provide authentication. On the other hand, it is well understood that BANs are also extremely vulnerable to various malicious attacks, which have not attracted abundant research attention so far. In this paper, an attack-resilient malicious node detection scheme (*BAN-Trust*) is proposed for wireless body area networks that are able to detect and cope with malicious attacks in BANs. The effectiveness and efficiency of the proposed BAN-Trust scheme is validated through extensive experiments.

I.INTRODUCTION

In recent years, wireless body area networks (BANs) emerge as a key technology to support various telehealth applications. A BAN is wireless networks that is generally composed of small wearable or implantable sensor nodes that are placed in, on or around a patient's body. To monitor the patients real-time health status, these sensors measure, process, and share the body's physiological signs (such as heart rate, blood pressure, blood glucose level, temperature, pH, respiration, oxygen saturation, etc.) via wireless communication without constraining the activities of the patient. Moreover, a data terminal (such as a hand-held device like a smart phone) is usually associated with the similar patient, which aggregates, processes, and transmits the sensor data to the healthcare providers.

Physicians and caregivers can then access these sensor data for real-time diagnosis and trigger treatment procedures if necessary. When compared to the traditional sensor networks, BANs generally deal with more important and sensitive medical data which has more strict requirements for security protection. Despite that various research works have been conducted to secure BANs, little research effort has been made to detect malicious nodes and evaluate trustworthiness in BANs, which can lead to very severe outcomes. For example, if the wireless telemetry interface of a cardiac patient's pacemaker is hacked by attackers and it starts reporting fake readings, then this can be life-threatening because the pacemaker may stop working because of the untrustworthy data. Therefore, in addition to the existing security solutions for BANs, it is also critical to identify and cope with malicious nodes so that BANs can be better secured. In this paper, an attack-resilient malicious node detection scheme named *BAN-Trust* is proposed to better secure BANs. In the BAN-Trust scheme, we detect malicious nodes in BANs based on the behaviors observed by nodes themselves as well as recommendations shared by other nodes.

In addition, the trustworthiness of nodes is also evaluated based on the behavior history. The problem of trust management and malicious node detection in BANs has attracted little attention so far.

II.PROBLEM STATEMENT AND RELATED WORK

The implantable medical devices (IMDs), including pacemakers, cardiac defibrillators, insulin pumps, neurostimulators, etc. utilize their wireless radios to deliver timely patient information, leading to a better health care monitoring system.mIMDs report their data to a data sink by wireless communication channels. The data sink can be an IMD designed to store data or a smart phone, which has the ability to communicate with a remote healthcare agency through cellular networks or the Internet. All those IMDs, called a Wireless Body Area Network (WBAN). Unlike conventional sensor networks, a WBAN deals with more sensitive and important patient information that has significant security, privacy, and safety concerns, which may prevent the wide adoption of this technology. Node authentication is the most fundamental step towards a BAN's initial trust establishment, key production, and consequent secure communications.

III.SYSTEM ARCHITECTURE

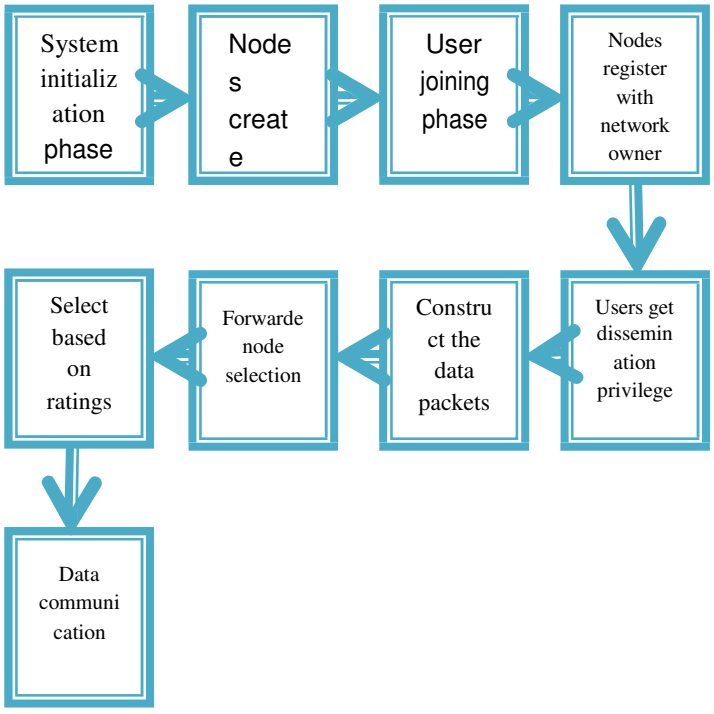

Figure.1.System architecture

Ns use two languages because simulator has two different kinds of things it needs to do.

On one hand, a detailed model of protocols requires a systems programming language which can efficiently influence bytes, packet headers, and implement algorithms that run over large data sets. For these tasks run-time velocity is important and turn-around time (run imitation, find bug, fix bug, recompile, re-run) is less key.

On the other hand, a large part of network research involves to some extent varying parameters or configurations, or quickly explore a number of scenario. In these cases, iteration time (change the replica and re-run) is more important. Since design runs once (at the beginning of the simulation), run-time of this part of the task is less significant.

Ns meets both of these needs with two languages, C++ and OTCl. C++ is fast to run but slower to change, making it appropriate for detailed protocol execution. OTCl runs much slower but can be changed very quickly (and interactively), making it ideal for replication configuration. ns (via tclcl) provides glue to make substance and variables appear on both languages.

IV.FUNCTIONAL SCENARIO

A) Network simulater

Ns are an object oriented simulator, written in C++, with an OTCl interpreter as a front end. The simulator wires a class hierarchy in C++ (also called the compiled pecking order in this paper), and a similar class hierarchy within the OTCl predictor (also called the interpret ladder in this paper). The two hierarchies are closely related to each other; from the user's perspective, there is a one-to-one correspondence between a class in the interpreted hierarchy and one in the compiled hierarchy. The root of this pecking order is the class Tcl Object. Users create new simulator objects through the interpreter; these objects are instantiated within the interpreter, and are closely mirrored by a equivalent object in the compiled hierarchy.

B) The Class Simulator

The overall simulator is describe by a Tcl class Simulator. It provides a set of interfaces for configuring a reproduction and for choosing the type of event scheduler used to drive the simulation. A reproduction draft generally begins by creating an request of this class and calling various methods to create nodes, topologies, and arrange other aspects of the simulation. A subclass of Simulator called Old Sim is used to support ns v1 backward compatibility.

C) Trace and Monitoring Support

There are a number of ways of collecting output or trace data on a reproduction. Generally, trace data is either display directly during implementation of the simulation, or (more usually) stored in a file to be post-processed and analyzed. There are two key but distinct types of monitoring capability currently supported by the simulator. The first, called traces, confirmation each individual packet as it arrives, departs, or is dropped at a link or queue. Trace substance are configured into a simulation as nodes in the network topology, usually with a Tcl "Channel" object addicted to them, representing the destination of collected data (typically a trace file in the current directory). The other types of objects, called monitor, record counts of various interesting quantities such as packet and byte arrivals, departure, etc.

D) Trace File Report

The trace support in OTCl consists of a number of specialized classes visible in OTCl but implemented in C++, combined with a set of Tcl helper procedures and classes defined in the ns library.

E) NS2 Structure Introduction

NS2 is an object sloping simulator, written in C++, with a Tcl interpreter as a front-end. The simulator wires a class hierarchy in C++ (also called the compile hierarchy), and a similar class hierarchy within the Tcl predictor (also called the interpret hierarchy).

The two hierarchies are directly related to each other; from the user's perspective, there is a one-to-one correspondence between a class in the interpreted chain of command and one in the compile hierarchy.

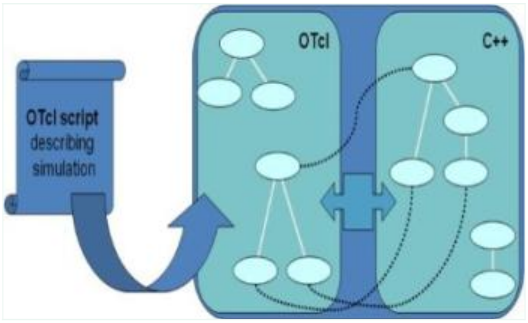

Figure.2. NS2 internal schematic diagram

Different kinds of belongings it needs to do:

1. Comprehensive simulations of protocols require a systems programming speech which can efficiently manipulate bytes, packet headers, and apply algorithms that run over large data sets. For these tasks run-time is important and turn-around time (run simulation, locate bug, fix bug, recompile, re-run) is less important. C++ is fast to run but slower to change, making it suitable for detailed protocol implementation.
2. A large part of network examine involves slightly varying parameters or configurations, or quickly exploring a number of scenarios. In these cases, iteration time (modify the copy and re-run) is more important. Since arrangement runs once (at the beginning of the simulation), run-time of this part of the task is less important. Tcl runs slower than C++ but can be changed very rapidly (and interactively), making it ideal for simulation configuration.

Users generate new simulator objects through the Tcl interpreter. These objects are instantiated within the predictor, and are closely mirrored by a corresponding object in the compile hierarchy. Class Tcl Object is the base class for most of the other classes in the interpreted and compiled hierarchies. Each object in the class Tcl Object is created by the user from within the predictor.

An equivalent shadow object is created in the compiled hierarchy. The two substances are closely linked with each other. The interpreted class hierarchy is automatically recognized through methods defined in the class Tcl Class. User instantiated substance is mirror through method define in the class Tcl entity. [4] proposed a system which is an innovative congestion control algorithm named FAQ-MAST TCP (Fast Active Queue Management Stability Transmission Control Protocol) is aimed for high-speed long-latency networks.

F) Delay and Packet Scheduling

Packet scheduling refers to the conclusion process used to choose which packets should be service or dropped.

Delays characterize the time required for a packet to traverse a link. The amount of point required for a packet to traverse a link is defined to be $\frac{s}{b} + d$ where s is the packet size (as recorded in its IP header), b b is the speed of the link in $\frac{bits}{sec}$, and d is the link wait in seconds.

Delays are defined in Link setback class in ~ns/delay.cc and the performance of the delay is in the recv () method. This method operates by receiving a packet, p, and scheduling two events.

G. Nodes and Packet Forwarding

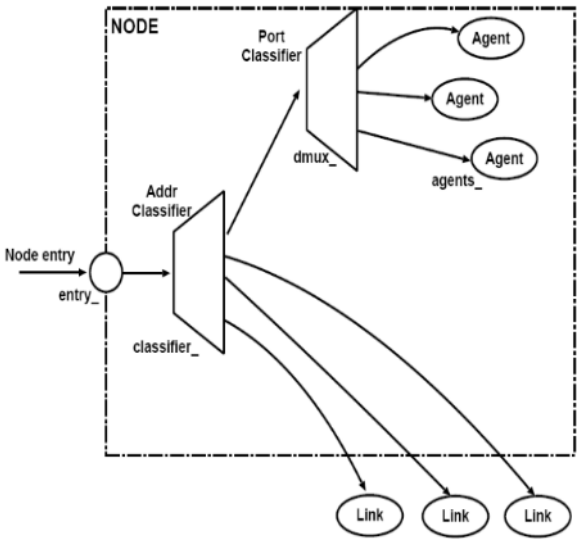

Figure.3. Node structure

Remember that each simulation require a single illustration of the class Simulator to control and operate that simulation. The class provides instance measures to create and manage the topology, and internally stores reference to each constituent of the topology. Here brought the instance measures in the class Node to access and operate on character nodes in each recreation.

V. RESULT AND DISCUSSION

A sensor can organize the access to the data it has produced by construct an access structure. Data are stored in cipher text arrangement at the data sink and the trust we put on the data sink is now drastically decreased as the information sink does not have the key to decrypt the stored cipher text. However, the proposal belongs to the asymmetric encryption family, which implies a high computational cost. The sensor nodes are associated with wireless link. The antenna nodes would transmit the data to the Base station nodes. The sensors nodes are assigned with slumber/awake duty cycles over period of time. The antenna nodes need to use the energy to send, obtain the data. The statement is enabled in the network among sensor node and base station, the performance of proposed method is analyzed. Based on the analyze results X-graphs are plotted.

Throughput, delay, energy consumption are the basic parameters considered here and X-graphs are plotted for these parameters. at last, the results obtained from this module is compared with third component results and comparison X-graphs are plotted. Form the assessment result, final RESULT is completed.

VI. Conclusion

In this paper, a novel attack-resilient malicious node detection scheme named BAN-Trust is proposed to address the security and trust concerns of wireless body area networks. In this scheme, the trustworthiness of BAN nodes is modeled and evaluated as two parts, namely functional trust and recommendation trust, respectively.

In addition, malicious nodes are also detected for BANs. To validate the proposed trust management scheme, extensive experiments have been conducted.

REFERENCES

1) G. Adomavicius and A. Tuzhilin, "Toward the next generation of recommender systems: a survey of the state-of-the-art and possible extensions," *IEEE Transactions on Knowledge and Data Engineering*, vol. 17, no. 6, pp. 734–749, June 2005

2) S. Buchegger and J.-Y. Le Boudec, "Performance analysis of the confidant protocol," in *MobiHoc '02: Proceedings of the 3rd ACM international symposium on Mobile ad hoc networking & computing*. New York, NY, USA: ACM, 2002, pp. 226–236.

3) J. S. Breese, D. Heckerman, and C. Kadie, "Empirical analysis of predictive algorithms for collaborative filtering," in *Proceedings of the Fourteenth Conference on Uncertainty in Artificial Intelligence*, ser.UAI'98. San Francisco, CA, USA: Morgan Kaufmann Publishers Inc., 1998, pp. 43–52.

4) Christo Ananth, S.Esakki Rajavel, I.AnnaDurai, A.Mydeen@SyedAli, C.Sudalai@UtchiMahali, M.Ruban Kingston, "FAQ-MAST TCP for Secure Download", International Journal of Communication and Computer Technologies (IJCCTS), Volume 02 – No.13 Issue: 01 , Mar 2014, pp 78-85

5) S. D. Kamvar, M. T. Schlosser, and H. Garcia-Molina, "The eigentrust algorithm for reputation management in p2p networks," in Proceedings of the 12th International Conference on World Wide Web, ser. WWW '03. ACM, 2003, pp. 640–651.

6) M. Li, W. Lou, and K. Ren, "Data security and privacy in wireless body area networks," *IEEE Wireless Communications*, vol. 17, no. 1, pp. 51–58, February 2010.

7) C. Piao, J. Zhao, and J. Feng, "Research on entropy-based collaborative filtering algorithm," in *Proceedings of 2007 IEEE International Conference on e-Business Engineering (ICEBE 2007)*, Oct 2007, pp. 213–220.

8) P. Resnick, N. Iacovou, M. Suchak, P. Bergstrom, and J. Riedl, "Grouplens: An open architecture for collaborative filtering of netnews," in *Proceedings of the 1994 ACM Conference on Computer Supported Cooperative Work*, ser. CSCW '94. ACM, 1994, pp. 175–186.

9) M. Raya, P. Papadimitratos, V. D. Gligor, and J.-P. Hubaux, "On data-centric trust stablishment in ephemeral ad hoc networks," in *Proceedings of the IEEE INFOCOM 2008*. IEEE, 2008, pp. 1238– 1246.

10) Y. Ren and A. Boukerche, "Performance analysis of trust-based node evaluation schemes in wireless and mobile ad hoc networks," in *Proceedings of 2009 IEEE International Conference onCommunications, ICC '09.*, june 2009, pp. 1–5.

11) R. Shaikh, H. Jameel, B. d'Auriol, H. Lee, S. Lee, and Y.-J. Song, "Group-based trust management scheme for clustered wireless sensor networks," *IEEE Transactions on Parallel and Distributed Systems*, vol. 20, no. 11, pp. 1698–1712, Nov 2009.

12) L. Shi, J. Yuan, S. Yu, and M. Li, "Ask-ban: Authenticated secret key extraction utilizing channel characteristics for body area networks," in *Proceedings of the Sixth ACM Conference on Security and Privacy in Wireless and Mobile Networks*, ser. WiSec '13. New York, NY, USA: ACM, 2013, pp. 155–166.

13) L. Shi, M. Li, S. Yu, and J. Yuan, "Bana: Body area network authentication exploiting channel characteristics," in *Proceedings of the Fifth ACM Conference on Security and Privacy in Wireless and Mobile Networks*, ser. WISEC '12. New York, NY, USA: ACM, 2012, pp. 27–38.

14) C. C. Tan, H. Wang, S. Zhong, and Q. Li, "Body sensor network security: An identity-based cryptography approach," in *Proceedings of the First M Conference on Wireless Network Security*, ser. WiSec '08. New York, NY, USA: ACM, 2008, pp. 148–153.

15) X. Zeng, R. Bagrodia, and M. Gerla, "Glomosim: a library for parallel simulation of large-scale wireless networks," *ACM SIGSIM Simulation Digest*, vol. 28, no. 1, pp. 154–161, 1998.