International Journal of Innovative Research in Computer Science & Technology (IJIRCST)
ISSN: 2347-5552, Volume-9, Issue-1, January 2022
https://doi.org/10.55524/ijircst.2022.10.1.13
Article ID IJIRD-1156, Pages 79-82
www.ijircst.org

Enhancement of Security in Wireless Sensor Network by Using Trust Evaluation and TCP/IP Based Technology

Rahul Das[1], and Dr. Mona Dwivedi[2]

[1]Research Scholar, Department of Computer Science, Mansarovar Global University, Billkisganj, Sehore, Madhya Pradesh, India
[2]Professor, Department of Computer Science, Mansarovar Global University, Billkisganj, Sehore, Madhya Pradesh, India

Correspondence should be addressed to Rahul Das; rahul.rr.das@gmail.com

ABSTRACT-Today Wireless network technology are widely used technology in many organizations. Wireless LANs transmit and receive data without physical channel means over the air so no need for a wired connection. For this radio frequency (RF) technology is used. Without any cables attached, a wireless network allows devices to remain linked to the network. The main advantage of wireless network is that it is typically cheaper, simpler, quicker to set up as wireless network does not require expensive wiring.
Mainly radio communication is used to implement wireless communication networks. At physical level of OSI model network structure this implementation takes place. Examples of wireless networks include cell phone networks, Wi-Fi local networks & terrestrial microwave networks. The advent of wireless sensor network has given birth to new kinds of routing algorithms and new security threats.

KEYWORDS-Wireless Sensor Network, Hacker, TCP/IP, Port, Socket, Cryptography.

I. INTRODUCTION

In computer network Wireless network is uses a connection that transfer data wirelessly with connecting network nodes. Various wireless network systems are

A. Terrestrial Microwave

The focused beam of a radio signal is transmitted by this technology that transmits from one antenna to another antenna that is also a ground-based microwave transmission type (figure 1). Generally, Microwaves are electromagnetic wave that has the frequency range from 1GHz to 1000 GHz.These waves are unidirectional waves where antennas are focused narrowly.

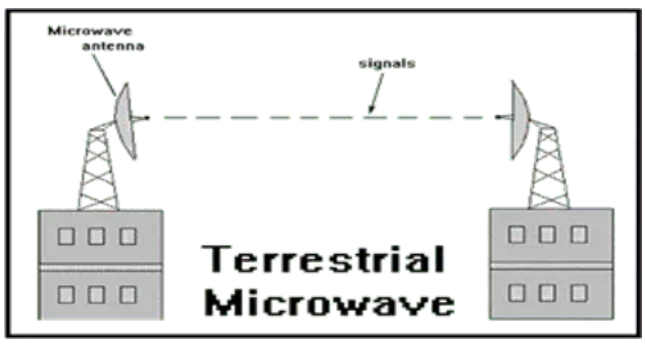

Figure 1: Terrestrial microwave

- Cellular & PCS systems use several radio communications technologies. Systems divide region covered into multiple geographic areas. Each area has a low-power transmitter or radio relay antenna device to relay calls from one area to next area.
- Radio & spread spectrum technologies: Spread spectrum is a technique used for transmitting radio or telecommunications signals. The meaning of the term represents to the practice of spreading the signal that was transmitted to occupy the available frequency spectrum for transmission. Noise reduction, security and resistance to jamming and interception are some advantages of spectrum spreading.

B. Transmission by Satellites

For broadcasting and receiving of signals Satellite (figure 2) Microwave Transmission System uses satellites These satellites are positioned in space and the signals are transmitted to space and it retransmits the signal to the appropriate location.

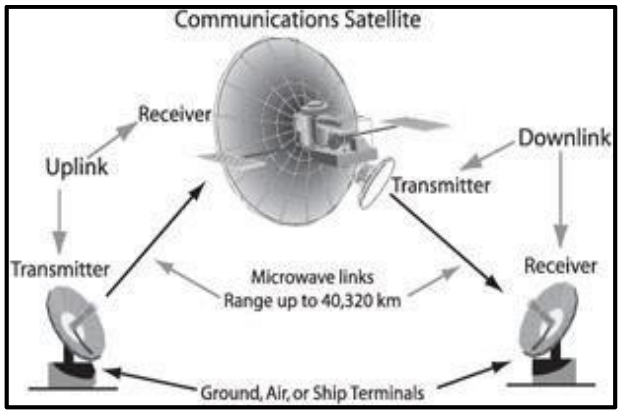

Figure 2: Satellite Communication

II. WIRELESS SENSOR NETWORK

Wireless sensor networks sometimes called wireless sensor and actuator networks (WSAN)[1][2] are spatially distributed autonomous sensors to monitor physical or environmental conditions, such as temperature, sound, pressure, etc. The most advanced modern networks are bi-directional, also activate control of sensor activity in different situations. Main motivation for the development of wireless sensor networks was military applications such as

battlefield surveillance; now a day such networks are widely used in many industrial and consumer applications, like industrial process monitoring and control, machine health monitoring, etc.

The WSN is made by many number of "nodes" – that may be from a few to several hundreds or even thousands, where each and every node is connected to one sensor. A sensor network node has typically many parts: a radio transceiver that has an internal antenna or connection that is connected to an external antenna, a microcontroller, for interfacing an electronic circuit with the sensors and an energy source, that are commonly a battery. The size of a sensor node might vary in size. Ranging from a few to hundreds of dollars, depending on the complexity of the individual sensor nodes the cost of sensor nodes is similarly variable.

Energy, memory, computational speed and communications bandwidth are the corresponding constraints on resources. From a simple star network to an advanced multi-hop wireless mesh network Topology can vary in the WSNs. Routing or flooding are the propagation technique between the hops of the network. In computer science and telecommunications wireless sensor networks are an active research area with so many workshops and conferences arranged each and every year, for example SenSys, EWSN and IPSN.

III. WIRELESS AD-HOC NETWORK

Presently Wireless Ad Hoc Networks has been ongoing research subject for decades. The wireless ad hoc networks involved into the survivable adaptive radio networks (SURAD) program. Ad hoc networks is used in battle field operations, health care monitoring, military applications and related research field. Some examples are Near-term digital radio (NTDR) program and the global mobile information systems (GloMo) program. As communication equipment and computers become more compact, a new type of industrial and commercial applications use wireless ad hoc networks. Wireless networks have become increasingly popular in the communication industry since 1970's. These networks provide mobile users with ubiquitous computing capability and information access regardless of the users' location. Infrastructure and infrastructure less networks are two types that are currently present in mobile wireless network. Fixed and wired gateways and the fixed Base-Stations are characteristics of infrastructure networks, through wires which are connected to other Base-Stations.

Within the range of a Base-Station each node is present. As mobile host travels out of range of one Base-Station and into the range of another, a "Hand-off" occurs and thus mobile host is able to continue communication seamlessly throughout the network. Wireless local area networks and Mobile Phone are example of this type. Mobile Ad-hoc Networks (MANET) is type of wireless network that have no fixed routers and all nodes have the capability of movement and connected with arbitrary manner in the network.

IV. SECURITY ISSUES IN AD HOC NETWORK

The most important things for all kinds of networks including the Wireless Ad Hoc Networks is Security. Security issues for Wireless Ad Hoc Networks are difficult rather than the security for fixed networks. This is happened due to frequent topology changes in the Wireless networks and system constraints in mobile devices. Small memory and bandwidth, low-power, and low battery power includes system constraints. Two factors that turn Wireless Ad-hoc Network architecture into highly hazardous architectures are Mobility of relaying nodes and the fragility or routes. Mobile Ad hoc Networks are not a flawed architecture, those are considered this, while we cannot see it used in practice is only because most of its applications are in military are totally wrong. Everybody knows that the core requirement for military applications dealing with trust and security. Especially for security sensitive applications security is the most important and vital issue for ad hoc networks. As we have mentioned before, in Mobile Ad-hoc Networks, security is difficult to implement because of t networks constrains and the rapidly topology changes. We found that there are two kinds of security related problem after investigation in the Mobile Ad-hoc Networks.

V. DESIGN METHODOLOGY

A. Socket Programming

The endpoint in an inter process communication is referred to as a socket, or a network socket for disambiguation. Since most communication among computers is primarily based on the Internet socket, an equivalent term used for this is Internet socket [10]. The transmission among sockets is organized by communications protocols, normally implemented in the operating system of the participate computers. Application programs write to and read from those sockets. Therefore, in network programming, a very important part is soc programming.

B. Client server Model

It is feasible for two network applications to start simultaneously; however, it's is impractical to require it. Therefore, it makes sense to de communicating network programs to carry out complementary operations required in series, in place of simultaneously. The server starts and waits to receive; the client executes second and sends the initial network packet to the server. After initial contact, either the client server is capable of sending and receiving information [11].

C. IP4 addresses:

IPv4 addresses have address code of 32 bits. They are denoted in decimal notation and dot, between them according to their class, each the 4 bytes that makes the 32 bits address are expressed as an integer value (0 – 255) and separated via a dot between them. For instance 159.39.57.28 is an example of an IP4 code/address, denoted in dotted decimal notation [12]. There is conversion function that convert bit address into a dotted decimal string and vice versa. With time changes even though the IP address is represented by a domain name example, uphill.Ucr.Edu. Several functions described here will allow you to convert from one form to another form (Magic provided by DNS!).The importance of IP addresses follows from the fact that each host on the Internet has a completely unique IP address. Thus, although the Internet is made from many networks of networks with many different types of architectures and transport mediums, it's the address which provides a cohesive structure so that (routing issues are

involved as well), any two hosts in the Network, can communicate or interact with each other.

Port

Sockets are UNIQUELY identified through Internet address, end-to-end protocol, and port number. That's why when a socket is created initially it is vital to match it with a valid IP address and a port number. In our labs we are able to working with TCP sockets. Many ports software objects to multiplex data between different applications [13]. When a host receives a packet, it travels up the protocol stack a finally reaches the application layers. Now consider a user, runs an ftp client, a telnet client, and a web browser simultaneously. To which client should the packet be delivered? Well part of the packet contains a value holding a port no; thus, this number determines to which application the packet should be delivered. So, while a client first attempts to contact a server, which port number should the client spec in many common services, a predefined standard port numbers are described for specific applications.

VI. PROPOSED MODEL

A. Trust Evaluation Module (TEM)

TEM is responsible for evaluating trustworthiness value of each communicating node through its packet forwarding, receiving and trans packet behaviour and estimates the probability of a node whether it is malicious or trustworthy (Figure 3). A node is declared as trustworthy if it forwards all the data to intend destination node and these information's are monitored which is then shared with other neighbouring nodes as direct or indirectly. Similarly, a malicious node is identified if it intentionally drops transmitting packets and record wrong information in t traffic profile by indicating correct number of received and forwarded packets Structure of WSN Clustering based trust estimation

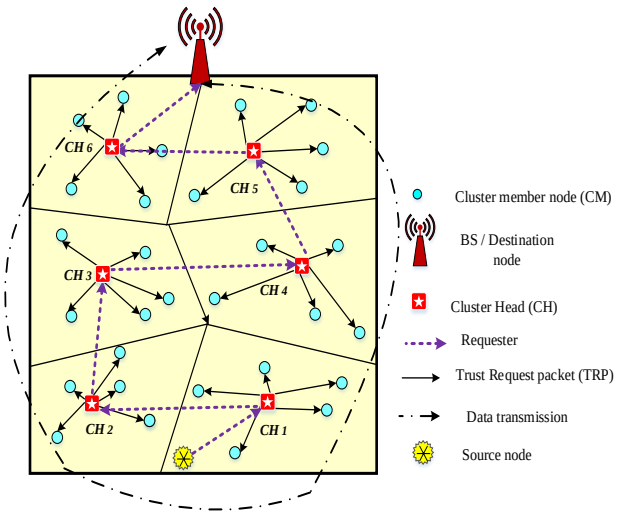

Figure 3: Structure of WSN Clustering based trust estimation

Trust model is one of the mathematical models gives opinion to one node to another at the way of transmission of information or data of network. The trust values also cause some uncertainty while taking decision based on the behaviour of nodes.

VII. SIMULATION ANALYSIS AND RESULTS

The proposed system is implemented and analysed in MATLAB for simulation and performance(Figure 4). For enhancing the security, the detect the malicious nodes and trust node are defined based on the computed trust values. Malicious nodes can be of Denial of Service (DoS attack, Bad-mouthing attack, on-off attack, collusion attack, Sybil attack and replication attack. An evaluation metrics used to evaluate t trust of each node in WSN are detection accuracy and energy consumption. The experimental simulation are based on this parameters the nodes are marked as Malicious and trusted according to the threshold value.

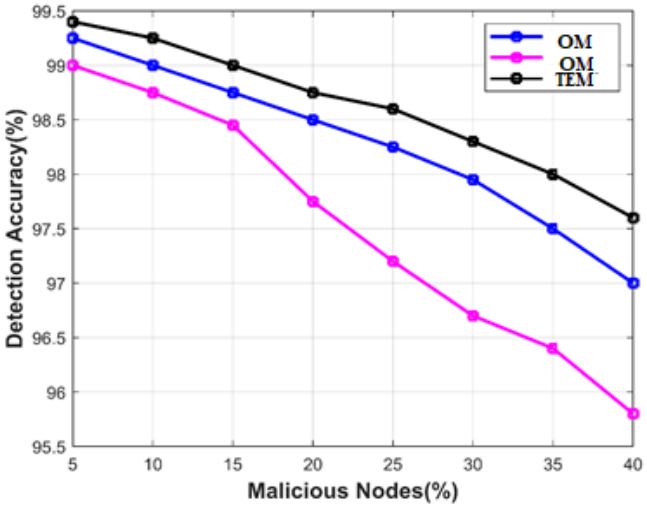

Figure 4: Comparison of Proposed and previous model.

VIII. CONCLUSION

Ad hoc network is a temporary network connection created for a specific purpose so the security of such system is must. There are several mechanisms to enhance the security of Ad hoc Network but they have some limitations. Our proposed system will overcome the previous limitation and enhance the security. The selection of trust-based CH and detecting malicious nodes in HWSN is a promising approach. Finally, our approach decreases in becoming a malicious node as a cluster head.

REFERENCE

[1] C.Siva Ram Murthy and B.Smanoj, " Ad Hoc Wireless Networks – Architectures and Protocols", Pearson Education, 2004.

[2] Feng Zhao and Leonidas Guibas, "Wireless Sensor Networks", Morgan Kaufman Publishers, 2004.

[3] C.K.Toh, "Ad Hoc Mobile Wireless Networks", Pearson Education, 2002.

[4] Thomas Krag and Sebastin Buettrich, "Wireless Mesh Networking", O'Reilly Publishers, 2007.

[5] Agi, I., Gong, L.: An empirical study of secure mpeg video transmissions. In: Proceedings of the Symposium on Network and Distributed System Security, pp. 137–144. IEEE Press, New York (1996)

[6] Baugher, M., McGrew, D., Naslund, M., Carrara, E., Norrman, K.: The secure real-time trans-port protocol (SRTP) (2004)

[7] Bergeron, C., Lamy-Bergot, C.: Complaint selective encryption for h.264/avc video streams. In: IEEE 7th

Workshop on Multimedia Signal Processing, pp. 1–4 (2005). doi: 10.1109/ MMSP.2005.248641
[8] Cheng, H., Li, X.: Partial encryption of compressed images and videos. IEEE Trans. Signal Process. 48(8), 2439–2451 (2000). doi: 10.1109/78.852023
[9] Chiaraluce, F., Ciccarelli, L., Gambi, E., Pierleoni, P., Reginelli, M.: A new chaotic algorithm for video encryption. IEEE Trans. Consum. Electron. 48(4), 838–844 (2002)
[10] Li, S., Zheng, X., Mou, X., Cai, Y.: Chaotic encryption scheme for real-time digital video. In: Real-Time Imaging VI. Proceedings of SPIE, vol. 4666, pp. 149–160 (2002)
[11] Lian, S., Liu, Z., Ren, Z., Wang, H.: Secure advanced video coding based on selective encryp-tion algorithms. IEEE Trans. Consum. Electron. 52(2), 621–629 (2006)
[12] Lian, S., Liu, Z., Ren, Z., Wang, H.: Commutative encryption and watermarking in video compression. IEEE Trans. Circuits Syst. Video Technol. 17(6), 774–778 (2007)
[13] Logik Bomb: Hacker's Encyclopedia (1997)

ABOUT THE AUTHORS

Rahul Das is a Research Scholar in Computer Science Department, Mansarovar Global University. Billkisganj, Sehore, Madhya Pradesh-466001.He is currently working as a teacher in the Department of Computer Science, Raja Narendralal Khan Women's college, Paschim Medinipur, West Bengal. He has received BCA degree in 2005 and Master's (MCA) under Vidyasagar University,2009 and B. Ed degree. He has 10 Years of teaching Experience in College. His research interest Security in Wireless Sensor Network.

Dr. Mona Dwivedi is currently working as an Assistant Professor in the Department of Computer Science at Mansarovar Global University, Billkisganj, Sehore, Madhya Pradesh, India. She received her M.Sc. and M.Phil. degree from Barkatullah University, Bhopal, M.P., India. Dr Dwivedi received her Ph.D. degree from Maulana Azad National Institute of Technology, Bhopal, India. Her research interest includes Green Computing, High Performance Computing, Wireless Sensor Networks, Numerical Analysis and Computational Modeling.