© INTERNATIONAL JOURNAL FOR RESEARCH PUBLICATION & SEMINAR
ISSN: 2278-6848 | Volume: 07 Issue: 06 | July – September 2016
Paper is available at www.jrps.in | Email : info@jrps.in

REVIEW ON SECURITY IN WIRELESS SENSOR NETWORK USING TCP/IP BASED TECHNOLOGY

[1]Sumit Tuteja, Research Scholar, Geeta Engineering College, Naultha Panipat.
[2] Mr. Nikhil Sharma ,Assistant Professor , Geeta Engineering College, Naultha Panipat,

Abstract: The rapid growth in Internet has made communication an organized and significantly imperative factor of computing. In the present society with the headway of mobile devices it has ended up being basic to stay online always. Wireless sensor networks alias wireless sensor and actuator networks (WSAN), [1][2] are the spatially dispersed autonomous sensors to screen physical or regular conditions, for instance, temperature, sound, weight, etcetera and to pleasantly send their data through the framework to a principal zone. The more present day frameworks are bi-directional, moreover engaging control of sensor development. The methodology of wireless sensor network has delivered new sorts of routing algorithms and new security threats also.

Keywords: Wireless sensor Network, Hacker, TCP/IP, PORT, SOCKET, CRYPTOGRAPHY.

[1] INTRODUCTION

Wireless system is any kind of computer network that utilized wireless information/data connections for connecting with network nodes [3, 4]. Wireless local area network technology are generally deployed and utilized in associations today. Utilizing radio frequency (RF) technology, wireless LANs transmit and get information over the air, limiting the requirement for wired associations. In this manner, wireless LANs combines information availability with client versatility. Wireless systems administration is a technique by which homes, media communications systems and venture establishments stay away from exorbitant procedure of bringing links into a building, or as an association between different hardware areas. Wireless communications networks are often executed & administered using radio communication. This execution happens at physical level of OSI model network structure. Examples of wireless systems incorporate cell phone systems, Wi-Fi local network systems and terrestrial microwave systems.

Various wireless network systems:-

1. Terrestrial microwave: – Terrestrial microwave communication utilizes Earth-based transmitters & receivers resembling satellite dishes. Terrestrial microwaves used in low-gigahertz range, which limits its communication to line-of-sight. Relay stations are spaced approx. 48 km apart [3, 4].
2. Cellular & PCS systems: - It use several radio communications technologies and divides region covered into numerous geographic areas. Each area has a low-power transmitter or radio relay antenna device to relay calls from one area to next area [3, 4].

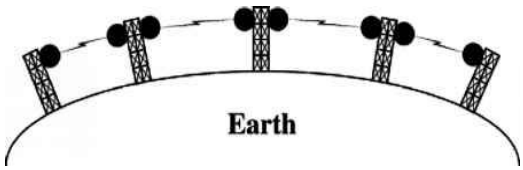

Fig. 1. Terrestrial Microwave [5]

3. Radio & spread spectrum technologies: – Wireless local area networks use a high-frequency radio technology like digital cellular technology and a low-frequency radio technology. Wireless LANs utilizes spread spectrum technology to enable communication between multiple devices in a limited area. IEEE 802.11 characterizes a typical kind of open-standard wireless radio-wave innovation known as Wi-Fi [3, 4].
4. Free-space optical communication: - It utilizes visible or invisible light in communication. Line-of-sight propagation is used, which limits physical positioning of communicating devices [3, 4].
5. Communications Satellites: – Satellites communicate via microwave radio waves, which are not deflected by Earth's atmosphere. Satellites are stationed in space, typically in geosynchronous orbit 35,400 km above equator. These Earth-orbiting systems are capable of receiving & relaying voice, data, & TV signals [3, 4].

Wireless sensor network

Wireless sensor networks sometime alias wireless sensor and actuator networks (WSAN),[1][2] are spatially distributed autonomous sensors to monitor physical or environmental conditions, for example, temperature, sound, pressure, etc. and to cooperatively pass their data through the network to a principle zone or area. The more modern systems are bi-directional,

© INTERNATIONAL JOURNAL FOR RESEARCH PUBLICATION & SEMINAR
ISSN: 2278-6848 | Volume: 07 Issue: 06 | July – September 2016
Paper is available at www.jrps.in | Email : info@jrps.in

also empowering control of sensor activity. The advancement of wireless sensor networks was spurred by military applications, for example, front line surveillance; today such networks are utilized in numerous industrial and consumer based applications, such as industrial process monitoring and control machine, health monitoring, and etcetera.

The WSN is built of "nodes" – from a couple to a few hundreds or even thousands, where each node is connected to one sensors. Each such wireless sensor network node has typically several parts: a radio transmitter and receiver with an internal antenna or connection to an external antenna, a microcontroller, an electronic circuit to interface with the sensors and an energy source, usually a battery or an embedded form of energy source. A sensor node may differ in size from that of a shoebox down to the size of a particle of dust, although functioning "motes" of genuine microscopic dimensions have yet to be created for future applications. The cost of sensor nodes is likewise factor, ranging from a few dollars to thousands of dollars, depending on the complexity and efficiency of the individual sensor nodes. Size and cost constraints in sensor nodes results in corresponding constraints on resources like memory, energy, computational speed and bandwidth. Topology of the Wireless sensor networks varies from a simple star network topology to an advanced multi-hop wireless mesh network topology. The propagation technique in the hops of the network can be routing or flooding. In computer science and telecommunications, wireless sensor network is an active area of research with various workshops and conferences arranged every year, like IPSN, SenSys, and EWSN.

[2] WIRELESS AD-HOC NETWORK

Ad hoc wireless networks are characterized as the classification of wireless networks that use multi-hop radio transferring and are capable of working without the help of any fixed infrastructure, hence they are alias infrastructure less networks. [6, 7]. Wireless mesh network system and wireless sensor network system are specific examples of wireless ad hoc networks [8]. The other type of wireless network is cellular network also known as infrastructure based network. The infrastructure networks have fixed and wired gateways like fixed Base-Stations that are connected to other Base-Stations with the help of wires. All nodes is within the range of a Base-Station. A Hand-off happens as mobile host travels from range of one Base-Station to the range of another and thus, mobile device is able to continue communication flawlessly throughout the network. Applications of this type of networks include wireless local area networks and Mobile Phone. The other type of wireless systems, infrastructure less networks, alias Mobile Ad-hoc Networks (MANET). These have no fixed routers, all nodes could be router, are capable of movement and can be connected. In Cellular System, the presence of base stations simplifies routing and resource management, and the routing decisions are made in a centralized manner with more information about the destination node. But in an ad hoc wireless network system, routing and resource management are done in a distributed manner in which all nodes coordinate among themselves to enable communication. It requires every node to be more intelligent so that it functions both as a network host for transmitting and receiving and as a network router for routing packets to and from other nodes. Wireless mobile nodes in an ad hoc wireless networks are more complex than their counterparts in cellular networks but they are easy to install and economical in operations, Ad hoc wireless networks, due to their fast and cost effective deployment, find applications in numerous areas, such as in military applications, computing, emergency operations, wireless mesh networks, wireless sensor networks, and in hybrid wireless network architectures.

[3] SECURITY ISSUES IN AD HOC NETWORK

Security is an important concern in all types of networks including the Wireless Ad Hoc Networks. It is clearly to see that the security issues for Wireless Ad Hoc Networks are troublesome than the ones for fixed wired networks [9]. This is due to the framework requirements in mobile devices as well as frequent topology switches in the Wireless networks. For instance System constraints like low-power, less memory, bandwidth and battery requirement.

Mobility of transmitting nodes and the fragility of routes turn the Wireless Ad-hoc Network architecture into highly perilous architectures. No entity is guaranteed to be available at every time and it is very difficult to rely on a centralized structure that could define network structure or even authentication. The people who consider the Mobile Ad hoc Networks are not an imprecise architecture and we cannot see its practical implementation in practice is only because most of its applications are in military are totally wrong. It is the fact that Wireless Mobile Ad hoc Networks originates from the military applications. But perhaps those people forgot about one of the most important thing: the Security! Everybody feels that the core requirement in military applications is trust and other is security. In other words, we have to say that security is the crucial issue in wireless ad hoc networks, mainly in the security sensitive applications.

As we have discussed before, in Mobile Ad-hoc Networks, security is hard to implement because of the networks constrains and the rapidly topology changes. After investigation, we found that there are two types of security related issues in these Wireless Networks.

© INTERNATIONAL JOURNAL FOR RESEARCH PUBLICATION & SEMINAR
ISSN: 2278-6848 | Volume: 07 Issue: 06 | July – September 2016
Paper is available at www.jrps.in | Email : info@jrps.in

[4] OBJECTIVE OF RESEARCH

1. Researcher proposes to design and analyze a new server side module and client side module to transfer multimedia contents for Ad-Hoc Network.
2. Researcher also proposes a novel Key independent and fast & selective video Encryption Technique for Confidentiality of video stream delivered over Ad-Hoc Network to end user.
3. Deployment & Integration of above two techniques simultaneously for providing Confidentiality & Authentication of Video Delivered or received over self-Deployed Ad-Hoc Network for Video on Demand Service.
4. To enhance the network security of Digital Data by adding New Security Mechanisms
5. Research proposes to design easy to use graphical user interface for Ad-Hoc Network.

[5] DESIGN METHODOLOGY

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 data transmission among sockets is organized by communications protocols, normally implemented in the operating system of the participating computers. Application programs write to and read from those sockets. Therefore, in network programming, a very important part is socket programming.

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 design communicating network programs to carry out complementary operations required in series, in place of simultaneously. The server start first and waits to receive; the client executes second and sends the initial network packet to the server. After initial contact, either the client or the server is capable of sending and receiving information [11].

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 of 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 are conversion function that convert a 32 bit address into a dotted decimal string and vice versa. With time changes even though the IP address is represented by a domain name, for 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 type of architectures and transport mediums, it's the IP address which provides a cohesive structures 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 are software objects to multiplex data between different applications [13]. When a host receives a packet, it travels up the protocol stack and 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 specify?, In many common

© INTERNATIONAL JOURNAL FOR RESEARCH PUBLICATION & SEMINAR
ISSN: 2278-6848 | Volume: 07 Issue: 06 | July – September 2016
Paper is available at www.jrps.in | Email : info@jrps.in

services, a predefined standard port numbers are described for specific applications.

[6] EXISTING RESEARCH

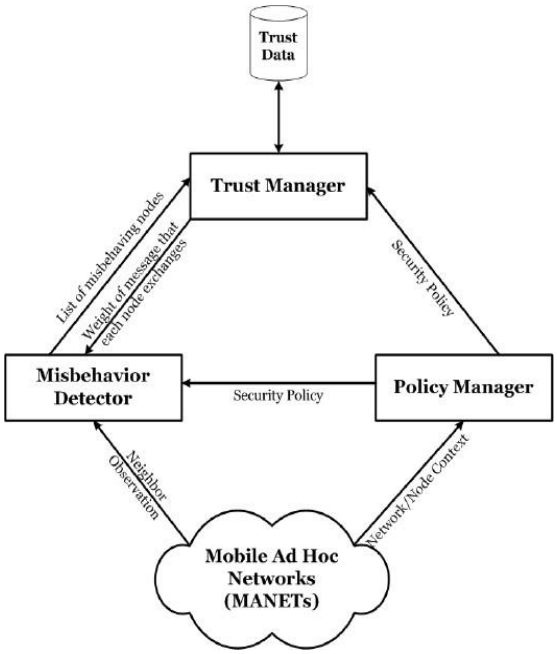

Fig. 2. System Architecture [14]

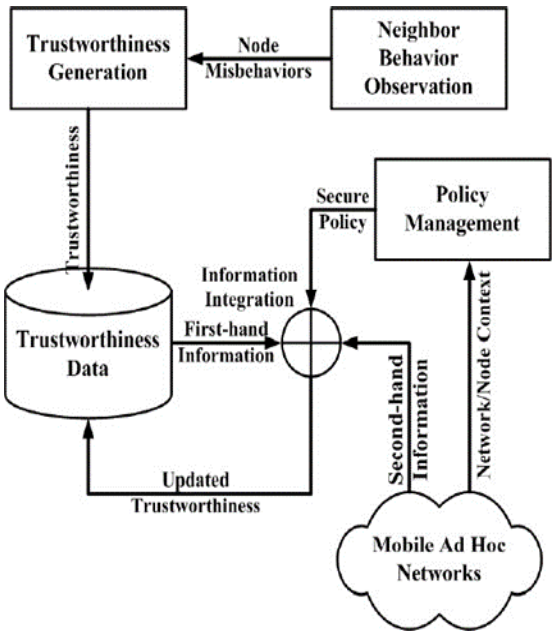

Fig. 3. Trust Management [14]

[7] DATA FLOW DIAGRAM OF PROPOSED MODEL

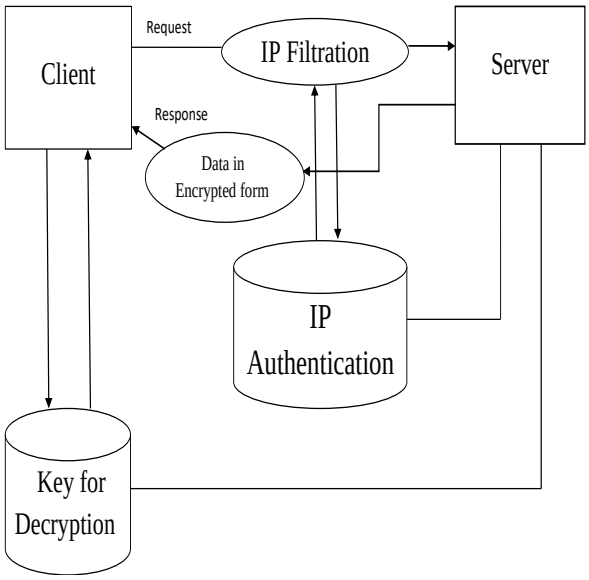

Fig. 4. Proposed Model with Enhanced Security

[8] 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.

REFERENCE

1. Sohraby, K., Minoli, D., and Znati, T., 2007, *Wireless sensor networks: technology, protocols and applications*, John Wiley & Sons, Inc., Hoboken, New Jersey, pp. 38-71.
2. Zhao, F. and Guibas, L. 2004, *Wireless Sensor Network*, Morgan Kaufman Publishers, Burlington, Massachusetts.
3. Benny, H., Kumar, C. S., Deepthi, D.V.V., Rao, S. K., and Raju, G. S.V.P., 2013 "Overcome of Router/Gateway Problems in Wireless Networks", *International Journal on Advanced Computer Theory and Engineering (IJACTE)*, vol. 2 (5), pp. 66-67.
4. Wikipedia Contributor's, 2016, "Wireless Networks",[online].Available:https://en.wikipedia.org/w/index.php?title=Wireless_network&oldid=721993952. [Accessed May 26, 2016].
5. Fisher Telecommunication Services, 2015,

"Terrestial Microwave", fishercom.xyz. [Online].Available:https://www.fishercom.xyz/division-multiplexing/terrestrial-microwave.html. [Accessed February 8, 2016].

6. C.Siva Ram Murthy and B.S.Manoj, 2004, *Ad Hoc Wireless Networks – Architectures and Protocols*, Pearson Education, Upper Saddle River, New Jersey.
7. C.K.Toh, 2002, *Ad Hoc Mobile Wireless Networks*, Pearson Education, Upper Saddle River, New Jersey.
8. Thomas Krag and Sebastin Buettrich, 2007, *Wireless Mesh Networking*, O'Reilly Publishers, Sebastopol, California.
9. Sarvesh Tanwar, Prema K.V., 2013,"Threats & Security Issues in Ad hoc network: A Survey Report", International Journal of Soft Computing and Engineering (IJSCE), vol.2 (6), pp.138-143.
10. Kalita, L., 2014, "Socket Programming", *International Journal of Computer Science and Information Technologies*, vol. 5 (3), pp. 4802-4807.
11. Wikipedia Contributors, 2015, "Client-Server Model", in Wikipedia. [Online].Available:https://en.wikipedia.org/w/index.php?title=Client%E2%80%93server_model&ol did=681622405.
12. Symantec, (2007), "Overview of IP addressing and subnetting", [Online]. Available:https://support.symantec.com/en_US/article.TECH82138.html [Accessed Feb. 3, 2016].
13. Wikipedia Contributors, 2016, "Port", in Wikipedia,[Online].Available:https://en.wikipedia.org/w/index.php?title=Port_(computer_networking)&oldid=700433568 [Accessed Jan 18, 2016].
14. Li, Wenjia & Joshi, Anupam & Finin, Tim. (2009), "Policy-Based Malicious Peer Detection in Ad Hoc Networks", Proceedings IEEE CSE'09, 12th IEEE International Conference on Computational Science and Engineering, pp.76-82. DOI: 10.1109/CSE.2009.289.