A Review on - Comparative Study of Issues in Cellular, Sensor and Adhoc Networks

Jayashree V. Shiral[1] and Bhushan N. Mahajan[2]

[1]Wireless Communication and Computing, G.H.R.C.E, Nagpur City, India
jayashreevshiral@yahoo.in
[2] Department of Computer Engineering, G.H.R.C.E, Nagpur City, India
anupcus123@gmail.com

ABSTRACT

A cellular network is an asymmetric radio network which is made up of fixed transceivers or nodes, maintain the signal while the mobile transceiver which is using the network is in the vicinity of the node. An ad-hoc network is a local area network (LAN) that is built spontaneously as devices connect.

Instead of relying on a base station to coordinate the flow of messages to each node in the network, the individual network nodes forward packets to and from each other.

This paper focuses on various issues in cellular, adhoc and sensor network. As issues proves helpful for forthcoming research, this paper work as a backbone to elaborate the various research areas.

KEYWORDS

Sensor Netwok , Cellular Network, Adhoc Network, Issues , Requirements

1. INTRODUCTION

A Cellular network is one of the radio network distributed over land areas called cells, each served by at least one fixed-location transceiver known as a cell site or base station .When these cells joined together provide radio coverage over a wide geographic areas. A wireless adhoc network is a decentralized type of wireless network. The network is adhoc because it does not depend on a preexisting infrastructure, such as routers in wired networks or access points in managed, infrastructure wireless networks.

2. WIRELESS SENSOR NETWORK

A wireless sensor network consists of group of sensors, or nodes, that are linked by a wireless medium to perform distributed sensing tasks. The sensors are assumed to have a fixed communication and a fixed sensing range, which can significantly vary depending on the type of sensing performed. It has received a greater interest in various applications such as disaster management, border protection, combat field reconnaissance, in military for security surveillance, structural health monitoring, industrial automation, civil structure monitoring, and monitoring the biologically hazardous places and in variety of applications.

David C. Wyld, et al. (Eds): CCSEA, SEA, CLOUD, DKMP, CS & IT 05, pp. 199–205, 2012.
© CS & IT-CSCP 2012 DOI : 10.5121/csit.2012.2221

A sensor network must be able to operate under very dynamic conditions. Specifically, our protocols must be able to enable network operation during start-up, steady state, and failure.The necessity of operation under these conditions is required because in most cases, the sensor network must operate unattended. Once the nodes have booted up and a network is formed, most of the nodes will be able to sustain a steady state of operation, i.e. their energy reservoirs are nearly full and they can support all the sensing, signal processing and communications tasks as required. In this mode, the bulk of the nodes will be formed into a multi-hop network. The node begin to establish routes by which information is passed to one or more sink nodes.

A Sink node is similar to head node which gather, control data collected by other sensor node. Also it is a sensor node with gateway functions to link to external networks such as the Internet and sensed information is normally distributed via the sink node.A sink node may be a long-range radio, capable of connecting the sensor network to existing long haul communications infrastructure. The sink may also be a mobile node acting as an information sink, or any other entity that is required to extract information from the sensor network. Although the multi-hop network can operate in both the sensor-to-sink or sink-to-sensor i.e broadcast or multi-cast modes. This will put significant strain on the energy resources of the nodes near the sink, making that neighborhood more susceptible to energy depletion and failure. Nodes may fail due to other reasons such as mechanical failure. When many nodes have failed, the MAC and routing protocols must accommodate formation of new links and routes to the sink nodes. This may require actively adjusting transmit powers and signaling rates on the existing links to reduce energy consumption, or rerouting packets through regions of the network where nodes have more energy left.

Sensor nodes are expected to operate autonomously in unattended environments and potentially in large numbers. Failures are susceptible in wireless sensor networks due to inhospitable, unstable environment and unattended deployment. The data communication and various network operations cause energy depletion in sensor nodes and therefore, it is common for sensor nodes to exhaust its energy completely and stop operating. This may cause connectivity and data loss during communication. Therefore, it is necessary that network failures are detected in advance and appropriate measures should be taken to sustain network operation. Connections to establish communication between nodes may be formed using media such as infrared devices or radios.

2.1. Issues in WSN Security

Energy efficiency: The requirement for energy efficiency suggests that in most cases computation is favoured over communication, as communication is three orders of magnitude

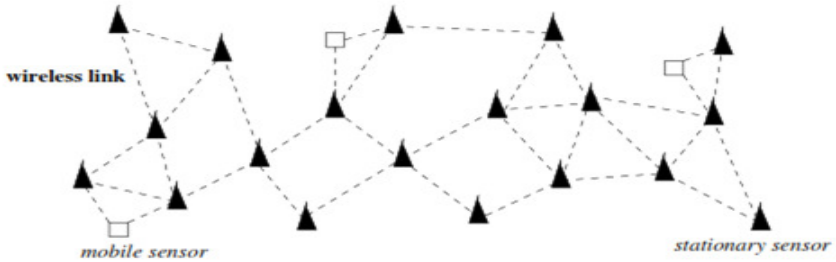

Figure 1. A Wireless Sensor Network

more expensive than computation. The requirement also suggests that security should never be overdone - on the contrary, tolerance is generally preferred to overaggressive

prevention. More computationally intensive algorithms cannot be used to incorporate security due to energy considerations.

- No public-key cryptography: Public-key algorithms remain prohibitively expensive on sensor nodes both in terms of storage and energy. No security schemes should rely on public-key cryptography. However it has been shown that authentication and key exchange protocols using optimized software implementations of public-key cryptography is very much viable for smaller networks.

- Physically tamperable: Since sensor nodes are low-cost hardware that are not built with tamper-resistance in mind, their strength has to lie in their number. Even if a few nodes go down, the network survives. The network should instead be resilient to attacks.

- Multiple layers of defence: Security becomes an important concern because attacks can occur on different layers of a networking stack as defined in the Open System Interconnect model. Naturally it is evident that a multiple layer of defence is required, i.e. a separate defence for each layer. The issues mentioned here are in general applicable to almost all sorts of domain irrespective of their traits.

2.2. Security Requirements in WSN

- Availability: Sensors are strongly constrained by many factors, e.g., limited computation and communication capabilities. Additional computations or communications consumes additional energy and if there is no more energy, data will not be available. Energy is another extremely limited resource in large scale wireless sensor networks. A single point failure will be introduced while using the central point scheme. This greatly threatens the availability of the network. The requirement of security not only affects the operation of the network, but also is highly important in maintaining the availability of the whole network. Moreover, wireless sensor networks are vulnerable to various attacks. The adversary is assumed to possess more resources such as powerful processors and expensive radio bandwidth than sensors. Equipped with richer resources, the adversary can launch even more serious attacks such as DoS attack, resource consumption attack and node compromise attack.

- Confidentiality: Data confidentiality is the most important issue in network security. These security services are achieved by cryptographic primitives as the building blocks. Confidentiality means that unauthorized third parties cannot read information between two communicating parties. A sensor network should not leak sensor readings to its neighbours. Especially in a military application, the data stored in the sensor node may be highly sensitive.

- Integrity and authenticity: Confidentiality only ensures that data can not be read by the third party, but it does not guarantee that data is unaltered or unchanged. Integrity means the message one receives is exactly what was sent and it was unaltered by unauthorized third parties or damaged during transmission. Wireless sensor networks use wireless broadcasting as communication method. Thus it is more vulnerable to eavesdropping and message alteration.

3. CELLULAR NETWORK

A Cellular network is one of the radio network distributed over land areas called cells, each served by at least one fixed-location transceiver known as a cell site or base station .When these cells joined together provide radio coverage over a wide geographic areas. Cellular networks provides the advantages such as increased capacity, reduced power use, large coverage area, reduced interference from other signals. In cellular architecture the network is partitioned into a virtual grid of cells to perform fault detection and recovery locally with minimum energy consumption . Figure 2. shows the cellular network.

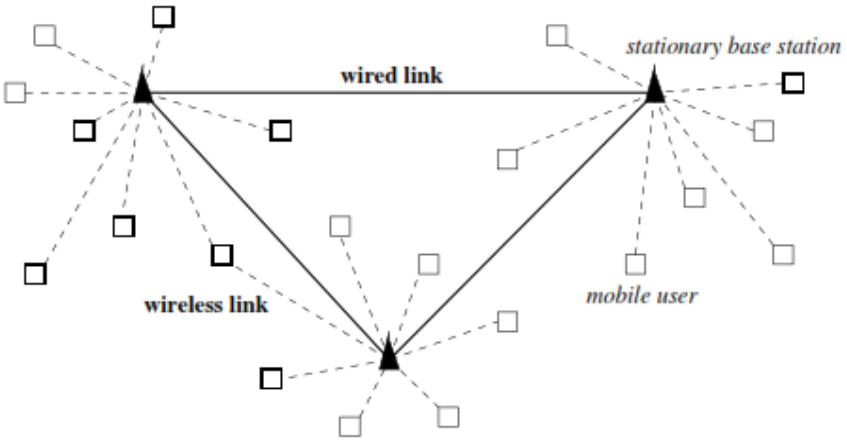

Figure 2. A Cellular Network

3.1. Security Issues in Cellular Network

- Authentication: Cellular networks have a large number of subscribers, and each has to be authenticated to ensure the right people are using the network. Since the purpose of 3G is to enable people to communicate from anywhere in the world, the issue of cross region and cross provider authentication becomes an issue.

- Integrity: With services such as SMS, chat and file transfer it is important that the data arrives without any modifications.

- Confidentiality: With the increased use of cellular phones in sensitive communication, there is a need for a secure channel in order to transmit information.

- Access Control: The Cellular device may have files that need to have restricted access to them. The device might access a database where some sort of role based access control is necessary.

- Mobile Devices: Cellular Phones have evolved from low processing power, ad-hoc supervisors to high power processors and full fledged operating systems. Some phones may use a Java Based system, others use Microsoft Windows CE and have the same capabilities as a desktop computer. Issues may arise in the OS which might open security holes that can be exploited.

- Web Services: A Web Service is a component that provides functionality accessible through the web using the standard HTTP Protocol. This opens the cellular device to variety of security issues such as viruses, buffer overflows, denial of service attacks etc.

- Location Detection: The actual location of a cellular device needs to be kept hidden for reasons of privacy of the user. With the move to IP based networks, the issue arises that a user may be associated with an access point and therefore their location might be compromised.

- Viruses And Malware: With increased functionality provided in cellular systems, problems prevalent in larger systems such as viruses and malware arise. The first virus that appeared on cellular devices was Liberty. An affected device can also be used to attack the cellular network infrastructure by becoming part of a large scale denial of service attack.

- Downloaded Contents: Spyware or Adware might be downloaded causing security issues. Another problem is that of digital rights management. User might download unauthorized copies of music, videos, wallpapers and games.

- Device Security: If a device is lost or stolen, it needs to be protected from unauthorized use so that potential sensitive information such as emails, documents, phone numbers etc. cannot be accessed.

4. ADHOC NETWORK

A wireless adhoc network is a decentralized type of wireless network. The network is adhoc because it does not depend on a preexisting infrastructure, such as routers in wired networks or access points in managed, infrastructure wireless networks. Instead, each node participates in routing by forwarding data for other nodes, and so the determination of which nodes forward data is made dynamically based on the network connectivity. A Mobile Adhoc Network (MANET) is an autonomous collection of mobile routers and associated hosts connected by bandwidth-constrained wireless links. Each node is viewed as a personal information appliance such as a personal digital assistant (PDA) fitted out with a fairly sophisticated radio transceiver. The nodes are fully mobile.

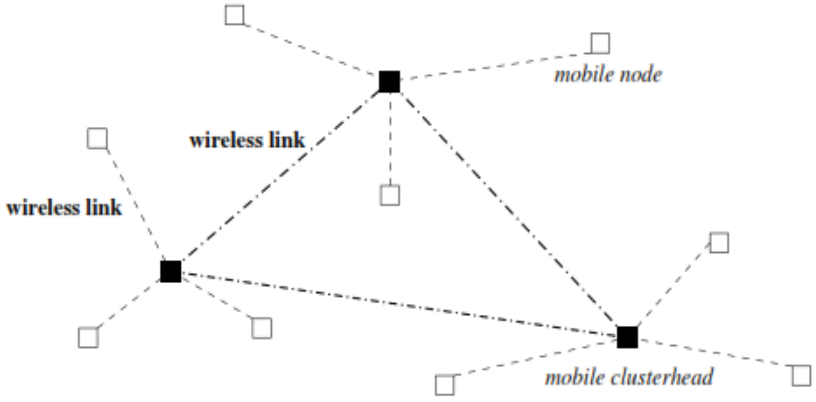

Figure 3. A Mobile Adhoc Network (MANET)

The network's wireless topology may change rapidly and unpredictably. Such a network may operate in a standalone fashion or may be connected to the larger Internet. Factors, such as variable wireless link quality, propagation path loss, fading, multiuser interference, power expended, and topological changes, significantly increase the complexity of designing network protocols for MANETs. Security, latency, reliability, intentional jamming, and recovery from failure are also the significant factors of concern. Figure 3. Shows the mobile adhoc network.

4.1. Security Issues in Adhoc Network

- Vulnerability of Channels: As in any wireless network, messages can be eavesdropped and fake messages can be injected into the network without the difficulty of having physical access to network components.

- Vulnerability of nodes: Since the network nodes usually do not reside in physically protected places, such as locked rooms, they can more easily be captured and fall under the control of an attacker.

- Absence of Infrastructure: Ad hoc networks are supposed to operate independently of any fixed infrastructure. This makes the classical security solutions based on certification authorities and on-line servers inapplicable.

- Dynamically Changing Topology: In mobile ad hoc networks, the permanent changes of topology require sophisticated routing protocols, the security of which is an additional challenge. A particular difficulty is that incorrect routing information can be generated by compromised nodes or as a result of some topology changes and it is hard to distinguish between the two cases.

4.2. Security Requirements for Adhoc Network

- Availability: Ensures survivability despite Denial Of Service (DOS) attacks. On physical and media access control layer attacker can use jamming techniques to interfere with communication on physical channel. On network layer the attacker can disrupt the routing protocol. On higher layers, the attacker could bring down high level services e.g.: key management service.

- Confidentiality: Ensures certain information is never disclosed to unauthorized entities.

- Integrity: Message being transmitted is never corrupted.

- Authentication: Enables a node to ensure the identity of the peer node it is communicating with. Without which an attacker would impersonate a node, thus gaining unauthorized access to resource and sensitive information and interfering with operation of other nodes.

- Non-repudiation: Ensures that the origin of a message cannot deny having sent the message.

- Non-impersonation: No one else can pretend to be another authorized member to learn any useful information.

- Attacks using fabrication: Generation of false routing messages is termed as fabrication messages. Such attacks are difficult to detect.

5. CONCLUSIONS

This paper proposed the comparison between sensor network, cellular network and adhoc network . Also this paper includes various security issues and requirements of the above networks. Also this issues and requirements will be helpful to beginners to elaborate their research work.

REFERENCES

[1] Zoran S. Bojkovic, Bojan M. Bakmaz, and Miodrag R. Bakmaz (2008), "Security Issues in WSN," International Journal Of Communications, Issue 1, Volume 2.

[2] Karan Singh, R. S. Yadav, Ranvijay (2007), "Review Paper On Ad Hoc Network Security", International Journal of Computer Science and Security", Issue 1, Volume 1.

[3] Kalpana Sharma, M.K. Ghose, Deepak Kumar, Raja Peeyush Kumar Singh, Vikas Kumar Pande (2010), "A Comparative Study of Various Security Approaches Used in Wireless Sensor Networks", International Journal of Advanced Science and Technology, Vol. 17.

[4] H. Yang, H. Luo, F. Ye, S. Lu, and L. Zhang (2004), "Security in mobile networks: challenges and solutions," IEEE Wireless Communications, vol. 11, no. 1, pp. 38-47.

[5] Roberto Di Pietro, Pietro Michiardi, Refik Molva (2007), "Confidentiality and Integrity for Data Aggregation in WSN using Peer Monitoring".

[6] Nandini. S. Patil, Prof. P. R. Patil (2010), "Data Aggregation in Wireless Sensor Network,"IEEE International Conference on Computational Intelligence and Computing Research, 2010.

[7] Li, Raghu Kisore Neelisetti, Cong Liu, and Alvin Lim (2010), "Efficient Multipath Protocol for WSN", International Journal of Mobile and Wireless, Vol 2, No.1.

[8] Simarpreet Kaur, and Leena Mahajan (2011),"Power Saving MAC Protocols for WSNs and Optimization of S-MAC Protocol", International Journal of Radio Frequency Identification and Wireless Sensor Networks.

[9] Heinrich Luecken, Thomas Zasowski, and Armin Wittneben," Synchronization Scheme for Low Duty Cycle UWB Impulse Radio Receiver"IEEE Transaction on Communication, April 2008.

First Author – Ms. Jayashree V. Shiral is doing M.E in Wireless Communication and Computing from G.H.R.C.E, Nagpur. She has completed her B.E in Information Technology from Priyadarshini Institute of Engineering and Technology, Nagpur.
Email id: [1]jayashreevshiral@yahoo.in

Second Author – Prof. Bhushan N. Mahajan received Diploma in mechanical engineering in 1999, A.M.I.E. [CSE] Engineering degree in 2007, BCA degree in 2007 and MCA degree in 2009 and Master of Engineering degree in WCC [CSE] in 2010 at GHRCE, Nagpur University, India. He has simulated various network scenarios using ns2 network simulator software. He is now working on energy and power management, motes reprogramming and various schedule development strategies in WSN. He has a special interest in topology modeling of ad-hoc network i.e. wireless sensor network and wireless mesh network. He is a software developer. He has created various WSN protocols and agents using C++ and TCL in NS-2.
Email-id: [2]anupcus123@gmail.com