IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

A Review On Wireless Network And Its Associated Aspects

Amruth V[1], Devaraj Verma C[2]

[1]Research Scholar, Jain Deemed to be University and Assistant Professor at Maharaja Institute of Technology, Mysore

[2]Professor, Artificial Intelligence, Jain Deemed to be University, Bangalore

Abstract

Recent advancement in the microelectromechanical systems (MEMS), microsystem technologies (MST), and wireless communications have enabled the rise of energy efficient, economical, and off-the-shelf devices which can transfer data in a favorable way without any additional communicational overhead. The wireless devices often called as motes are now used in several wireless applications such as battle front monitoring, industrial process superintendence, industrial equipment performance monitoring and so on. In this paper we are trying to highlight the necessary information related to Wireless network, difference between wired and wireless network, attacks in Wireless Network, Localization, Ad hoc Networks and its topology.

Keywords: Wireless Network, Localization, Beacon node, Ad hoc Network

I. Introduction

The wireless devices work autonomously to perform its desired tasks such as monitoring leaks, temperature, pressure, vibrations, sound, and so on. These information's are systematically collected at regular intervals and stored or passed to the required central authority. Each device is equipped with tiny electrical parts such as radio transmitter and receiver for transmitting and receiving information from the neigh- boring wireless devices, a microcontroller unit for performing the computational work, an energy harvesting device such as battery to make the device work wireless, and the necessary senor chips.

II. Wireless Networks

Wireless networks differ significantly from traditional wired networks. Wireless networks requires dense node arrangement and cooperation and association with its neighboring wireless devices. A wireless network need not rely to physical cables to establish connection between devices. Because of this feature it has several advantages such as high efficiency, flexibility, portability, and economical to use. Wireless networks has several advantages as well as disadvantages when compared to wired network. Table 1 shows the comparison between wired and wireless networks.

Table 1: Wired vs Wireless Networks Comparison

S.No.	Type	Wired Network	Wireless Network
1	Mobility	Limitless	Fixed to an endpoint
2	Reconfigurations	Easy to reconfigure	Complex and expensive
3	Reliability	Varied results	Better results
4	Interference	Critical concern	No interference
5	Environment	Can introduce noise	No impact
6	Security	Less secure	Better secured than wireless
7	Speed	Slightly slower	Faster than wireless
8	Troubleshooting	Complex	Straightforward
9	Deployment cost	Low	Very expensive

A. Attacks in Wireless Networks

Securing each node in the wireless network is a must to provide a reliable system. An attack on a single node can bring down the entire wireless system. In the presence of malicious nodes, the ultimate goal of any wireless network is to provide privacy, honesty, genuineness, and accessibility of all essential information to qualified receivers.

Because of the node scalability and economical advantage the wireless networks continue to expand. The advancements in algorithms and software technologies has enabled the wireless network to capture big date which can be further processed to extract useful information [1]. The wireless network must protect sensitive information acquired or recorded from attackers. Several wireless network still use conventional ways to secure the network, and to provide a reliable communicational channel. In order to provide security against information stealing, researchers have developed several end to end protection techniques, one such technique is Se- cure Sockets Layer (SSL) [2]. SSLs goal is to provide integrity, authenticity and confidentiality of information that are exchanged between the wireless networks.

The wireless networks are not so secure when compared with wired networks [3]. The wireless networks are vulnerable towards eavesdropping, jamming or interference, packet sniffing, denial of service and man-in-the-middle attacks [3]. This has spurred the need for securing the wireless network against attacks.

The following parameters of wireless networks makes it difficult to stay secured with the help of conventional security mechanism:

- Cost Factor: The wireless devices are less expensive devices and cannot be equipped with high computational specifications. The energy consumption should be at the minimal rate so that the wireless devices will be available longer.
- Environment: The environment in which the wireless network is placed is not physically secure. The wireless network is mostly deployed in isolated places such as forest, and mountains. These pose the risk of physical attacks on the wireless devices present in the network.
- Communication: The medium though which the wireless devices communicate are open, anyone can establish communication if the bandwidth is identified. This make it easy for the attacker to attack any device in the wireless network.

The current security techniques are still not able to identify few attacks in the wire- less network, and advanced techniques are required to provide uninterrupted service of the wireless network in the presence of malicious devices. When an adversary node gains control of a vulnerable device in the wireless network, the attacker can launch internal attacks, reducing the wireless system's reliability.

B. Localization

During the initial deployment of a wireless network, each nodes are provided with their location reference. This is done either manually or the sensor nodes automatically calculate the distance with the help of GPS devices attached to it. Global positioning system (GPS) [4] is mostly used in identifying the location coordinates of a mobile node. It identifies the location with the help of 31 GPS satellites that around the Earth. A total of four satellites (3) satellites to identify the 3d position, 1 for adjusting the local clock uncertainty) are required to identify the location of a mobile node. Figure 1 shows the working of a GPS receiver installed in a wireless device. If GPS receivers are to be installed for each node in a dense network will increase the deployment cost, and GPS will not work effectively in an indoor and underwater environment [5].

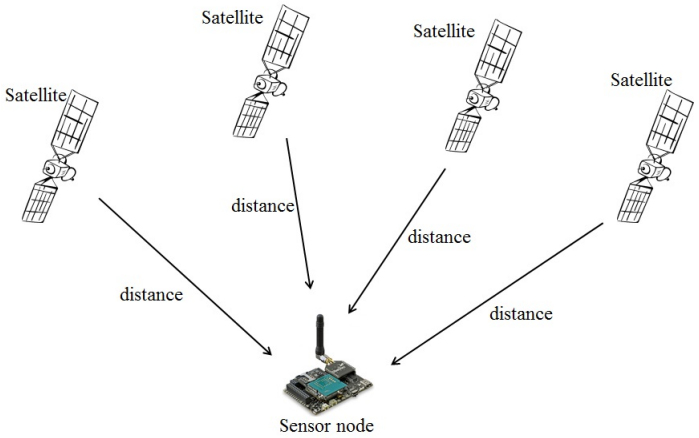

Figure 1: Working of GPS receiver installed in a wireless device.

To maintain a harmonious location identification of the mobile node, distributed localization schemes came into existence. Distributed localization schemes can over- come the drawbacks of GPS in an indoor and underwater environment. The mobile node that wants to find out its location reference starts by acquiring its range from three or more intermediate nodes, which then estimate the current location using trilateration technique. Installing a GPS device or manually computing the location may be impractical in the context of a large network due to the high cost and labour needed, respectively. To overcome this, each wireless nodes are made to identify their locations with the help of neighboring nodes [6].

B.1 Beacon Nodes

The process of identifying a wireless node's position with the help of its neighboring nodes is called a coordinated localization. The coordinated localization happens with the help of a special node known as beacon nodes. The beacon nodes are wireless devices in the network and it knows its current location, this is done by either setting up a GPS receiver in the beacon node or by manually configuring the location information into the beacon node. During the deployment of wireless sensor network, few sensor nodes are made configured with their location reference either manually or using GPS. These nodes act as the beacon nodes and the other nodes localize themselves with the support of beacon nodes.

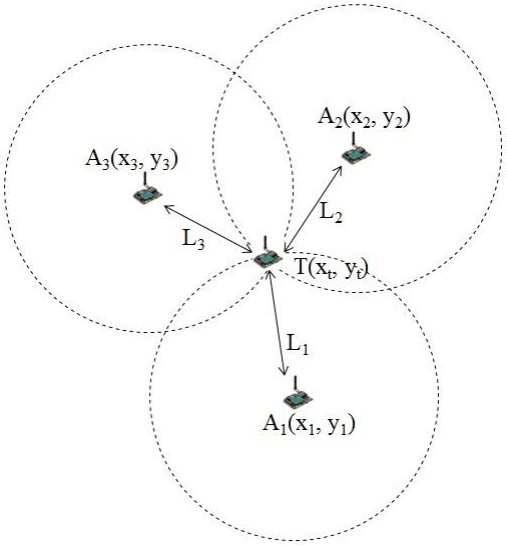

Figure 2: A typical localization process using beacon nodes.

Figure 2 shows a typical example of localization process using beacon nodes. the beacon nodes A_1, A_2, and A_3 are placed at the location coordinates (x_1, y_1), (x_2, y_2), and (x_3, y_3), respectively. L_1, L_2, and L_3 are the distance measurements between the new node N and the neighboring beacon nodes, respectively and the new node computes its location coordinates by using trilateration technique. We explain in detail about trilateration technique in our later section. Useful techniques such as TDoA, ToF or ToA, and RSSI are used to identify the distance measurements between the new node and its neighboring beacon nodes.

The steps involved in a typical localization process using RSSI ranging technique, is as follows:

1. A node that wants to initialize a communication sends a request to the neigh- boring nodes using the node's antenna.
2. The RSSI component in the neighboring nodes are responsible for extracting the RSSI measurements from each packet, and forwards the collected RSSI measurements to the beacon node.
3. The beacon node collects the entire RSSI measurements from the neighboring nodes and forwards the collected information to the identifier.
4. The identifier checks for any suspicion in the received packets and transmits its analysis to the neighboring nodes.
5. The collected RSSI measurements along with the analysis are shared with other three or more beacon nodes to perform a coordinated malicious beacon node identification.

B.2 Attacks during Localization

The salient features to perform a coordinated localization are localization precision, energy savings, and protection against attacks. There are extensive research carried out in the field of localization precision and energy efficiency. And in the recent decade, securing the localization phase has drawn the attention of researchers. A wireless node would not be able to identify its location in the presence of attackers.

The key metrics required to perform a successful localization is as follows:

- Beacon Node Availability: The beacon node must be available round the clock to assist a wireless node to localize.
- Beacon Node Integrity: The information provided by the beacon node must be secure and error free. A wireless node would be able to localize if the information provided by the beacon node is tampered.

- Authorization: Only authorized nodes can act as beacon node and help in assisting other wireless nodes during localization.
- Authentication: The authorized beacon nodes must be able to authenticate them to assist in localization.
- Disownment: Either the beacon node or the wireless node should not deny the information that were sent and received during localization.
- Privacy: Either the beacon node or the wireless node should not share the current localization information to other wireless nodes.

If an attacker or a malicious node tries to tamper any of the mentioned metrics, the wireless node will not be able to identify its correct location information. This creates a confusion in the system as the wireless node will not be able to perform its responsibilities. An attack during localization can be categorized into two types, insider attack, and outsider attack.

The insider attack occurs when a node in the wireless networks becomes malicious. The insider attack can also have access to authentication and authorization information of the wireless system. The insider attack can damage the wireless system at an alarming rate. Whereas in the outsider attack, the attacker can either physically capture the node or perform signal attenuation or amplification attacks to reduce localization accuracy. The outsider attack does not impact the wireless system much as compared to insider attack.

There are several localization algorithms such as trilateration, triangulation, and multilateration that can be used for identifying the location of a wireless node. The localization algorithms are discussed in brief in the later sections. These localization protocols face a small shortcoming in-spite of its popularity among wireless networks. During localization the nodes assume that the location information provided by the beacon nodes are true, and to have an efficient localization process valid location information's are required.

The localization accuracy deteriorate considerably in the presence of cheating or malicious beacon nodes. An attacker can also attack a beacon node and make the beacon node provide false location information or a compromised beacon nodes can introduce inaccuracies in the localization process by providing false location information or by manipulating the distance measurements. Figure 3 shows how a malicious beacon node reduces the consistency of the localization process causing the new node to compute false location reference.

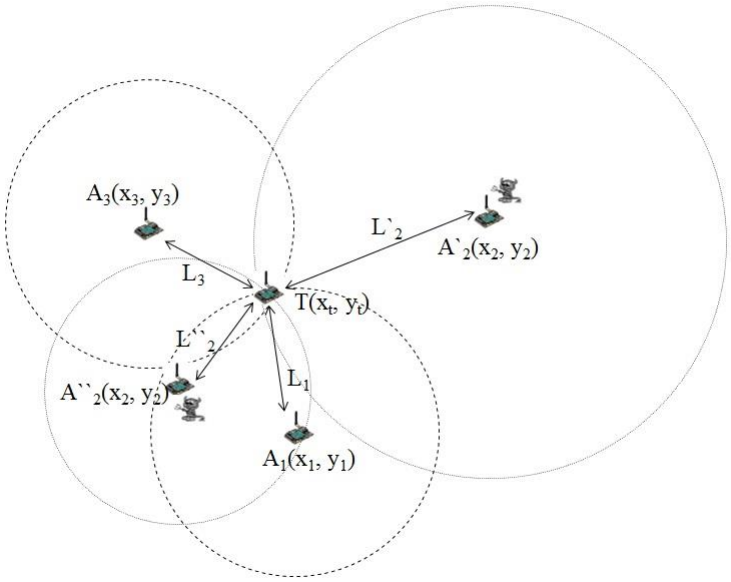

Figure 3: Impact of fraudulent beacon nodes during localization.

C. Ad Hoc Networks

Ad hoc networks has the vital state of the art trend in several research [7]. For the past 50 years notable research is happening in the field of ad hoc networks. The increase of low-cost wireless devices, and its easy accessibility and availability, elevated the interest of mobile computing communities.

The ad hoc network can be related back to the early 1970s where the Packet Ra- dio Network (PRNET) was introduced to provide well- grounded communication in a movable infrastructure, and in the early 1980s the Survivable Radio Network (SURAN) project was initiated to to provide a reliable communication in the field of mobile ad hoc networks (MANETs) [8]. These were developed to provide a reliable communication for military operations, in a decentralized combative environment such as battlefield, and aircraft carrier.

Portable mobile computers and open-source software (OSS) boosted the need for ad hoc networks in the early 1990s. The standardization of MANET routing protocols [9] spurred the growing interest of researchers in the field of MANETs. Similarly, several research advancements simulated the developments in the field of MANETs and its applications in wide number of areas such as emergency services, defense, e- commerce, entertainment, and education. Standalone/independent infrastructures and self-organizing features have made MANETs the suitable choice for applications that require information sharing, communication, and mobility. A typical example of MANET is shown in figure 4

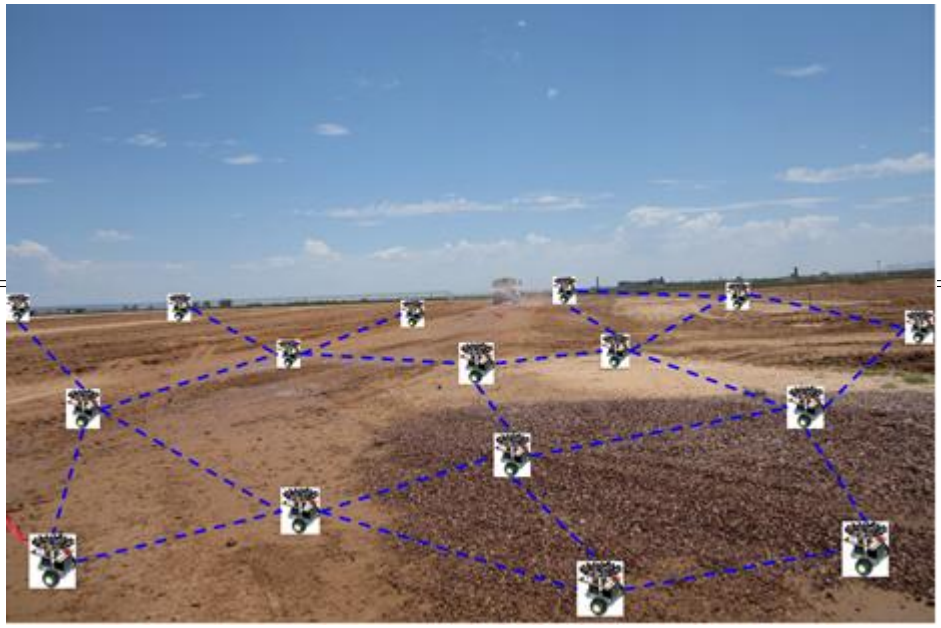

Figure 4: A typical example of MANET.

The ad hoc networks has several advantages as well as disadvantages when compared to cellular networks. Table 2 lists the advantages and disadvantages of ad hoc networks over cellular network.

C1 Network Topology

Ad hoc network follows a decentralized infrastructure for communication. When a wireless device wants to communicate with another wireless device in the network, the communication happens with the help of the peer node. A centralized system is not required to aid communication. Whereas in a wireless sensor network [10], all the

Table 2: Cellular vs Ad Hoc Network Comparison

S.No.	Cellular Network	Ad hoc network
1	Centralized routing	Distributed routing
2	Few nodes in the network are stationary such as base station	No stationary nodes in the network
3	Static network topology	Dynamic network topology
4	Expensive and time consuming deployment	Economical and rapid deployment
5	Stable connection	Patchy connectivity
6	Less packet loss during message transfer	Packet loss slightly higher

nodes are connected to a central monitoring system. The central monitoring system is required for data collection, for providing security mechanism, and so on. Figure 5 shows typical difference between centralized infrastructure and decentralized infrastructure, in wireless networks.

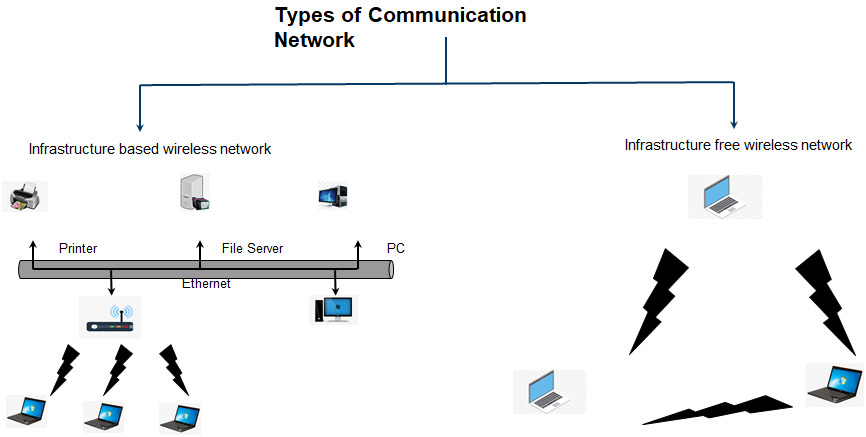

Figure 5: Centralized vs decentralized infrastructure.

In few cases, the ad hoc network would be associated to a static infrastructure, for acquiring Internet access. An ad hoc network can be created on the fly in the highways, where each vehicle on the highway act as the nodes. The vehicles can communicate with other vehicles to spread traffic and road information. This type of ad hoc network is called Vehicular ad hoc networks (VANETs) [11]. Multi- hop communication scheme can be used in an ad hoc network to provide message transfer in a dense network. Another distributed application architecture that used

ad hoc networks is peer-to-peer computing [12]. Peer-to-peer networks enhances the reliability, adaptability, performance and efficiency of a wireless network.

C2 Ad Hoc Communication

A typical example of how a communication happens between two nodes in an ad hoc network is shown in figure 1.6. The communication between two devices happens with the help of its neighbor. Each neighboring nodes act as router to transfer the data from sender to receiver, in a multihop manner [13].

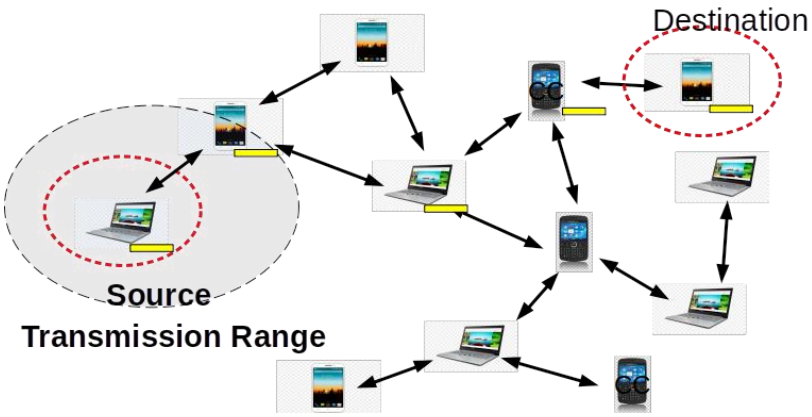

Figure 1.6: Ad hoc network communication.

The data exchange between the wireless nodes are initiated with the help of routing. In MANETs, routing is of two types proactive and reactive [14]. Proactive is a table driven routing technique and reactive is source-initiated on-demand-driven routing technique. Table driven routing will not be preferred while the mobility of the network is high, and reactive routing is used instead. Reactive routing in MANETs is generally initiated using few broadcasting schemes, and multipoint relay (MPR) broadcasting scheme [15] is believed to be the effectual and uncomplicated scheme. As MANETs are infrastructure-less network, the messages/data is transferred with the help of intermediate nodes [16].

References

[1] M. Ndiaye, G. P. Hancke, and A. M. Abu-Mahfouz, "Software defined network- ing for improved wireless sensor network management: A survey," Sensors, vol. 17, no. 5, p. 1031, 2017.

[2] A. Freier, P. Karlton, and P. Kocher, "The secure sockets layer (ssl) protocol version 3.0," RFC 6101, Tech. Rep., 2011.

[3] X. Huang, M. R. Ahmed, D. Sharma, and H. Cui, "Protecting wireless sensor networks from internal attacks based on uncertain decisions," in 2013 IEEE Wireless Communications and Networking Conference (WCNC). IEEE, 2013, pp. 1854–1859.

[4] B. Hofmann-Wellenhof, H. Lichtenegger, and J. Collins, Global positioning system: theory and practice. Springer Science & Business Media, 2012.

[5] J. Kuriakose, V. Amruth, A. Sandesh, V. Abhilash, G. P. Kumar, and K. Nithin, "A review on mobile sensor localization," in International Sym- posium on Security in Computing and Communication. Springer, 2014, pp. 30–44.

[6] J. Kuriakose, S. Joshi, R. V. Raju, and A. Kilaru, "A review on localization in wireless sensor networks," in Advances in signal processing and intelligent recognition systems. Springer, 2014, pp. 599–610.

[7] T. Qiu, N. Chen, K. Li, D. Qiao, and Z. Fu, "Heterogeneous ad hoc networks: Architectures, advances and challenges," Ad Hoc Networks, vol. 55, pp. 143–152, 2017.

[8] J. A. Freebersyser and B. Leiner, "A dod perspective on mobile ad hoc net- works," in Ad hoc networking, 2001, pp. 29–51.

[9] F. T. Al-Dhief, N. Sabri, S. Fouad, N. A. Latiff, and M. A. A. Albader, "A review of forest fire surveillance technologies: Mobile ad-hoc network rout- ing protocols perspective," Journal of King Saud University-Computer and Information Sciences, vol. 31, no. 2, pp. 135–146, 2019.

[10] J. Yick, B. Mukherjee, and D. Ghosal, "Wireless sensor network survey," Com- puter networks, vol. 52, no. 12, pp. 2292–2330, 2008.

[11] M. M. Hamdi, L. Audah, S. A. Rashid, A. H. Mohammed, S. Alani, and A. S. Mustafa,

"A review of applications, characteristics and challenges in vehicular ad hoc networks (vanets)," in 2020 International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA). IEEE, 2020, pp. 1–7.

[12] S. Asghari and N. J. Navimipour, "Resource discovery in the peer to peer networks using an inverted ant colony optimization algorithm," Peer-to-Peer Networking and Applications, vol. 12, no. 1, pp. 129–142, 2019.

[13] C. Buratti and R. Verdone, "End-to-end throughput of ad hoc multi-hop net- works in a poisson field of interferers," IEEE/ACM Transactions on Network- ing, vol. 25, no. 5, pp. 3189–3202, 2017.

[14] B. P. Maratha, T. R. Sheltami, and K. Salah, "Performance study of manet routing protocols in vanet," Arabian Journal for Science and Engineering, vol. 42, no. 8, pp. 3115–3126, 2017.

[15] T. K. Saini and S. C. Sharma, "Flexible multipoint relay selection for suit- able route in mobile ad hoc networks," Journal of Ambient Intelligence and Humanized Computing, pp. 1–14, 2020.

[16] J. Kuriakose and S. Joshi, "Secured mpr node selection in the presence of cheating nodes," International Journal of Trust Management in Computing and Communications, vol. 3, no. 3, pp. 246–268, 2016.

[17] M. A. Al-Ammar, S. Alhadhrami, A. Al-Salman, A. Alarifi, H. S. Al-Khalifa, A. Alnafessah, and M. Alsaleh, "Comparative survey of indoor positioning technologies, techniques, and algorithms," in 2014 International Conference on Cyberworlds. IEEE, 2014, pp. 245–252.