Wireless Sensor Network: Security Vulnerabilities Challenges, Design Principles And Performance Comparison Of Two On-Demand Routing Protocols For Ad Hoc Networks.

Priyanka Manhas[1] (Student)
Department of Computer Science & Engineering.
Chandigarh University (Gharuan, Mohali) India
priyankamanhas36@gmail.com

Parminder Kaur[2](Asstt. Prof.)
Department of Computer Science & Engineering.
Chandigarh University (Gharuan, Mohali) India
parminder.cu@gmail.com

Abstract-The significant advances of hardware manufacturing technology and the development of efficient software algorithms make technically and economically feasible a network composed of numerous, small, low-cost sensors using wireless communications, that is, a wireless sensor network (WSN). Security is becoming a major concern for WSN protocol designers because of the wide security-critical applications of WSNs. Ad hoc networks are characterized by multihop wireless connectivity, frequently changing network topology and the need for efficient dynamic routing protocols. We compare the performance of two prominent on-demand routing protocols for mobile ad hoc networks: Dynamic Source Routing (DSR) and Ad Hoc On-Demand Distance Vector Routing (AODV). The collaborative nature of industrial wireless sensor networks (IWSNs) brings several advantages over traditional wired industrial monitoring and control systems, including self-organization, rapid deployment, flexibility, and inherent intelligent-processing capability. In this regard, IWSN plays a vital role in creating a highly reliable and self-healing industrial system that rapidly responds to real-time events with appropriate actions. In this paper, first, technical challenges and design principles are introduced in terms of hardware development, system architectures and protocols, and software development and also define how WSN differs from wired network and other wireless network and also basic information about the WSN and its security issues compared with wired network and other wireless networks is discoursed.

Key Words- Security, Security Mechanism, Vulnerabilities, Wireless Sensor Network.

1 Introduction

In today's competitive industry marketplace, the companies face growing demands to improve process efficiencies, comply with environmental regulations, and meet corporate financial objectives. Given the increasing age of many industrial systems and the dynamic industrial manufacturing market, intelligent and low-cost industrial automation systems are required to improve the productivity and efficiency of such systems [6], [28]. Traditionally, industrial automation systems are realized through wired communications. However, the wired automation systems require expensive communication cables to be installed and regularly maintained, and thus, they are not widely implemented in industrial plants because of their high cost [29]. Therefore, there is an urgent need for cost-effective wireless automation systems that enable significant savings and reduce air-pollutant emissions by optimizing the management of industrial systems. One of the key issues rising from switching to wireless communication lies in security; while an air gap is among the most effective security measures in wired networks, wireless communication is not as easy to isolate from attack. The security issues in MANETs are more challenging than those in traditional wired computer networks and the Internet. Providing security in sensor networks is even more difficult than in MANETs due to the resource limitations of sensor nodes and security concerns remain a serious impediment to widespread adoption of these WSNs [27]. An *ad hoc* network, mobile nodes communicate with each other using multihop wireless links. There is no stationary infrastructure; for instance, there are no base stations. A *mobile ad hoc networking* (MANET) working group [2] has also been formed within the Internet Engineering Task Force (IETF) to develop a routing framework for IP-based protocols in ad hoc networks. Our goal is to carry out a systematic performance study of two dynamic routing protocols for ad hoc networks: the *Dynamic Source Routing* protocol (DSR) [3, 4] and the *Ad Hoc On-Demand Distance Vector* protocol (AODV) [5, 6].

DSR and AODV share an interesting common characteristic they both initiate routing activities on an *on demand* basis. This *reactive* nature of these protocols is a significant departure from more traditional *proactive*

protocols, which find routes between all source-destination pairs regardless of the use or need for such routes. The key motivation behind the design of on-Demand protocols is the reduction of the routing load. High routing load usually has a significant performance impact in low-bandwidth wireless links. While DSR and AODV share the on-demand behavior [7] in that they initiate routing activities only in the presence ofdata packets in need of a route, many of their routing mechanics are very different. In particular, DSR uses source routing, whereas AODV uses a table-driven routing framework and destination sequence numbers. DSR does not rely on any timer based activities, while AODV does to a certain extent. One of our goals in this study is to extract the relative merits of these mechanisms. The motivation is that a better understanding of the relative merits will serve as a cornerstone for development of more effective routing protocols for mobile ad hoc networks.

The rest of the article is organized as follows: In section 2, we briefly review the DSR and AODV protocols. In section 3, review the technical challenges and corresponding design directions, respectively. Finally, this paper is concluded in Section 4.

2 DESCRIPTION OF DSR AND AODV.

2.1 Dynamic Source Routing (DSR)

The key distinguishing feature of DSR [3, 4] is the use of *source routing*. That is, the sender knows the complete hop-by-hop route to the destination. These routes are stored in a *route cache*. The data packets carry the source route in the packet header. When a node in the ad hoc network attempts to send a data packet to a destination for which it does not already know the route, it uses a *route discovery* process to dynamically determine such a route. DSR makes very aggressive use of source routing and route caching. No special mechanism to detect routing loops is needed. Several additional optimizations have been proposed and have been evaluated
to be very effective by the authors of the protocol [7], as described in the following:

1. **Salvaging:** An intermediate node can use an alternate route from its own cache when a data packet meets a failed link on its source route.
2. **Gratuitous Route Repair:** A source node receiving an RERR packet piggybacks the RERR in the following RREQ. This helps clean up the caches of other nodes in the network that may have the failed link in one of the cached source routes.
3. **Promiscuous listening:** When a node overhears a packet not addressed to itself, it checks whether the packet could be routed via itself to gain a shorter route. If so, the node sends a *gratuitous* RREP to the source of the route with this new, better route. Aside from this, promiscuous listening helps a node to learn different routes without directly participating in the routing process.

2.2 Ad-Hoc On Demand Distance Vector Routing (AODV)

AODV [5, 6] shares DSR's on-demand characteristics in that it also discovers routes on an *as needed* basis via a similar route discovery process. However, AODV adopts a very different mechanism to maintain routing information. It uses traditional routing tables, one entry per destination. AODV uses sequence numbers maintained at each destination to determine freshness of routing information and to prevent routing loops [5]. These sequence numbers are carried by all routing packets. An important feature of AODV is the maintenance of timer-based states in each node, regarding utilization of individual routing table entries. A routing table entry is *expired* if not used recently. A set of predecessor nodes is maintained for each routing table entry, indicating the set of neighboring nodes which use that entry to route data packets. The recent specification of AODV [6] includes an optimization technique to control the RREQ flood in the route discovery process. It uses an *expanding ring search* initially to discover routes to an unknown destination. In the expanding ring search, increasingly larger neighborhoods are searched to find the destination.

3 TECHNICAL CHALLENGES AND DESIGN DIRECTIONS.

While WSNs come from wireless and ad-hoc networks. Some of the sensor network application require wireless and ad-hoc techniques. Although many algorithms and protocols have been proposed for traditional wireless ad-hoc network and they are not well suited for unique feature and application of sensor networks. Important distinction exist between ad-hoc networks and sensor networks greatly effect the system designs including security designs. The difference are as the following:

AD-HOC NETWORKS	SENSOR NETWORKS
Number of nodes in Ad-hoc network can not be several order of magnitude.	Number of nodes in sensor network can be several order of magnitude are higher.
Ad-hoc networks are not densely deployed	Sensor networks are densely deployed
Topology of Ad-hoc networks can not change frequently	Topology of sensor network can change very frequently due to node failure, joining and mobility
Ad-hoc networks are very rarely prone to failure	Sensor networks are prone to failure, due to its hostile environmental harsh deployment environments and energy constraints.
Ad-hoc networks based on point to point communication	Sensor nodes broadly used in broadcast communication.
Ad-hoc networks do not have power constraint	Sensor nodes are limited in power, computational capacity and memory
Ad-hoc networks have their own global identification ID	Sensor nodes do not have global identification ID. Because of large amount of overhead and large number of sensors.
Ad-hoc networks have more bandwidth as comparative to sensor networks	Sensor networks have limited bandwidth
Ad-hoc networks are not easy to compromised.	Sensor networks are easy to compromised
No power, energy , bandwidth, hardware constraint for Ad-hoc networks	Use of low power consumption. Sensor node carry limited, generally irreplicable power sources.

3.1 Challenges

Sensor network design in influenced by many factors which include: *fault tolerance , scalability, production cost, hardware constraint.* Sensor networks may consist of many different type of sensors, such as seismic, low sampling rate magnetic, thermal, visual, infrared, acoustic and radar, which can monitor temperature, humidity, vehicular movement, lighting condition, pressure, soil makeup, noise levels etc.

1. **Fault tolerance:** *Some sensor nodes may fail or be blocked due to lack of power, have physical* damage or environmental interference. The failure of sensor nodes should not affect the overall task of the sensor network. This is reliability of fault tolerance issue. The protocols and algorithms may designed to address the level of fault tolerance required by the sensor networks.
2. **Scalabilty:** Number of sensor nodes deployed in studying a phenomenon may be in the order of hundreds or thousands. The new scheme is able to work with this no. of nodes. They must also utilize the high density nature of the sensor networks. The number of nodes in a region can be used to indicate the node density. The node density depend upon the application in which the sensor nodes are deployed.
3. **Production cost:** As sensor network consist of large no. of sensor nodes. The cost of a single node is very important to justify the overall cost of the network. If the cost of the network is more
4. expensive than deploying traditional sensors, then the sensor network is not cost justified. As a result the cost of a sensor node has to be kept low.
5. **Hardware constraints:** Sensor node comprising of four main omponents: *Sensing Unit, Processing Unit, Transceiver Unit And Power Unit.*

Where sensing units are composed of two subunits: sensors or ADCs(Analog to digital converters). The analog signals produced by the sensors based on the observed phenomenon are converted to digital signals by the ADC, and then fed in to the processing units.

Processing unit which is generally associated with a small storage unit, manages the procedures that make the sensor node collaborate with the other nodes to carry out the assigned sensing tasks.

A transceiver unit connects the node to the network. The transceiver unit of sensor nodes may be a passive or active optical devices in smart dust motor a radio frequency device(RF)

The most important component of the sensor node is power unit. Power units may be supported by a power scavenging units such as solar cells.

They may also have application dependent additional components such as *location finding system, power generater and a mobilizer.*

1. **Resource Constraints:** The design and implementation of IWSNs are constrained by three types of resources: a) energy; b) memory; and c) processing. Constrained by the limited physical size, sensor nodes have limited battery energy supply [6]. At the same time, their memories are limited and have restricted computational capabilities.
2. **Dynamic Topologies And Harsh Environmental Conditions:** In industrial environments, the topology and connectivity of the network may vary due to link and sensor-node failures. Furthermore, sensors may also be subject to RF interference, highly caustic or corrosive environments, high humidity levels, vibrations, dirt and dust, or other conditions that challenge performance [28]. These harsh environmental conditions and dynamic network topologies may cause a portion of industrial sensor nodes to malfunction [7].
3. **Quality-Of-Service (Qos) Requirements:** The wide variety of applications envisaged on IWSNs will have different QoS requirements and specifications. The QoS provided by IWSNs refers to the accuracy between the data reported to the sink node (the control center) and what is actually occurring in the industrial environment. In addition, since sensor data are typically time-sensitive, e.g., alarm notifications for the industrial facilities, it is important to receive the data at the sink in a timely manner. Data with long latency due to processing or communication may be outdated and lead to wrong decisions in the monitoring system.
4. **Data Redundancy:** Because of the high density in the network topology, sensor observations are highly correlated in the space domain. In addition, the nature of the physical phenomenon constitutes the temporal correlation between each consecutive observation of the sensor node.
5. **Packet Errors And Variable-Link Capacity:** Compared to wired networks, in IWSNs, the attainable capacity of each wireless link depends on the interference level perceived at the receiver, and high bit error rates are observed in communication. In addition, wireless links exhibit widely varying characteristics over time and space due to obstructions and noisy environment. Thus, capacity and delay attainable at each link are location-dependent and vary continuously, making QoS provisioning a challenging task.
6. **Security***:* Security should be an essential feature in the design of IWSNs to make the communication safe from external denial-of-service (DoS) attacks and intrusion. IWSNs have special characteristics that enable new ways of security attacks. Passive attacks are carried out by eavesdropping on transmissions including traffic analysis or disclosure of message contents. Active attacks consist of modification, fabrication, and interruption, which in IWSN cases may include node capturing, routing attacks, or flooding.
7. **Large-Scale Deployment And Ad Hoc Architecture:** Most IWSNs contain a large number of sensor nodes (hundreds to thousands or even more), which might be spread randomly over the deployment field. Moreover, the lack of predetermined network infrastructure necessitates the IWSNs to establish connections and maintain network connectivity autonomously.
8. **Integration With Internet And Other Networks:** It is of fundamental importance for the commercial development of IWSNs to provide services that allow the querying of the network to retrieve useful information from anywhere and at any time. For this reason, the IWSNs should be remotely accessible from the Internet and, hence, need to be integrated with the Internet Protocol (IP) architecture. The current sensor-network platforms use gateways for integration between IWSNs and the Internet [2]. Note that although today's sensor networks use gateways for integration between IWSNs and the Internet, the sensor nodes may have IP connectivity in the future [18].

3.2 Design Goals

To deal with the technical challenges and meet the diverse IWSN application requirements, the following design goals need to be followed. Though there are varieties of challenges in sensor networks, here we focus on different security issues and possible remedies of those. Though security is a very important issue in WSN, due to various resource limitations and the salient features of a

WSN, the security design for such networks is significantly challenging.

1. **Low-Cost And Small Sensor Nodes:** Compact and low cost sensor devices are essential to accomplish large scale deployments of IWSNs. Note that the system owner should consider the cost of ownership (packaging requirements, modifications, maintainability, etc.), implementation costs, replacement and logistics costs, and training and servicing costs as well as the per unit costs all together [9].
2. **Scalable Architectures And Efficient Protocols:** The IWSNs support heterogeneous industrial applications with different requirements. It is necessary to develop flexible and scalable architectures that can accommodate the requirements of all these applications in the same infrastructure. Modular and hierarchical systems can enhance the system flexibility, robustness, and reliability. In addition, interoperability with existing legacy solutions, such as fieldbus- and Ethernet-based systems, is required.
3. **Secure Design:** When designing the security mechanisms for IWSNs, both low-level (key establishment and trust control, secrecy and authentication, privacy, robustness to communication DoS, secure routing, resilience to node capture) and high-level (secure group management, intrusion detection, secure data aggregation) security primitives should be ddressed [20]. In addition, because of resource limitations in IWSNs, the overhead associated with security protocols should be balanced against other QoS performance requirements.
4. **Data Fusion And Localized Processing:** Instead of sending the raw data to the sink node directly, sensor nodes can locally filter the sensed data based on the application requirements and transmit only the processed data, i.e., in network processing. Thus, only necessary information is transported to the end-user and communication overhead can be significantly reduced.
5. **Application-Specific Design:** In IWSNs, there exists no one-size-fits-all solution; instead, the alternative designs and techniques should be developed based on the application-specific QoS requirements and constraints.
6. **Self-Configuration And Self-Organization:** In IWSNs, the dynamic topologies caused by node failure/mobility/ temporary power-down and large-scale node deployments necessitate self-organizing architectures and protocols. Note that, with the use of self-configurable IWSNs, new sensor nodes can be added to replace failed sensor nodes in the deployment field, and existing nodes can also be removed from the system without affecting the general objective of the application.
7. **Fault Tolerance And Reliability:** In IWSNs, based on the application requirements, the sensed data should be reliably transferred to the sink node. Similarly, the programming/retasking data for sensor operation, command, and queries should be reliably delivered to the target sensor nodes to assure the proper functioning of the IWSN. However, for many IWSN applications, the sensed data are exchanged over time-varying and error prone wireless medium. Thus, data verification and correction on each communication layer and self-recovery procedures are extremely critical to provide accurate results to the end-user.
8. **Resource-Efficient Design:** In IWSNs, energy efficiency is important to maximize the network lifetime while providing the QoS required by the application. Energy saving can be accomplished in every component of the network by integrating network functionalities with energy efficient protocols, e.g., energy-aware routing on network layer, energy-saving mode on MAC layer, etc.
9. **Time Synchronization:** In IWSNs, large numbers of sensor nodes need to collaborate to perform the sensing task, and the collected data are usually delay-sensitive [2], [9]. Thus, time synchronization is one of the key design goals for communication protocol design to meet the deadlines of the application. However, due to resource and size limitations and lack of a fixed infrastructure, as well as the dynamic topologies in IWSNs, existing time synchronization strategies designed for other traditional wired and wireless networks may not be appropriate for IWSNs. Adaptive and scalable time-synchronization protocols are required for IWSNs.

4 CONCLUSION

The IWSNs have the potential to improve productivity of industrial systems by providing greater awareness, control, and integration of business processes. Despite of the great progress on development of IWSNs, quite a few issues still need to be explored in the future. For example, an efficient deployment of IWSNs in the real world is highly dependent on the ability to devise analytical models

to evaluate and predict IWSNs performance characteristics, such as communication latency and reliability and energy efficiency. However, because of the diverse industrial-application requirements and large scale of the network, several technical problems still remain to be solved in analytical IWSN models. We have compared the performance of DSR and AODV, two prominent on-demand routing protocols for ad hoc networks. DSR and AODV both use on-demand route discovery, but with different routing mechanics. In particular, DSR uses source routing and route caches, and does not depend on any periodic or timer-based activities. DSR exploits caching aggressively and maintains multiple routes per destination. AODV, on the other hand, uses routing tables, one route per destination, and destination sequence numbers, a mechanism to prevent loops and to determine freshness of routes. The general observation from the simulation is that for application-oriented metrics such as delay and throughput, DSR outperforms AODV in less "stressful" situations (i.e., smaller number of nodes and lower load and/or mobility). We believe that mechanisms to expire routes and/or determine freshness of routes in the route cache will benefit DSR's performance significantly. We believe that mechanisms to expire routes and/or determine freshness of routes in the route cache will benefit DSR's performance significantly. Since AODV keeps track of actively used routes, multiple actively used destinations also can be searched using a single route discovery flood to control routing load. In general, it was observed that both protocols could benefit:

1. From using congestion-related metrics (e.g., queue lengths) to evaluate routes instead of emphasizing the hop-wise shortest routes.
2. By removing "aged" packets from the network. The aged packets are typically not important for the upper layer protocol, because they will probably be retransmitted.

These stale packets do contribute unnecessarily to the load in the routing layer. Other open issues
include optimal sensor-node deployment, localization, security, and interoperability between different IWSN manufacturers. Many security issues in WSNs remain open and we expect to see more research activities on these exciting topics in the future.

REFERENCES

[1] N. Aakvaag, M. Mathiesen, and G. Thonet, "Timing and power issues in wireless sensor networks—An industrial test case," in *Proc. Int. Conf. Parallel Process. Workshops*, 2005, pp. 419–426.

[2] V. C. Gungor and F. C. Lambert, "A survey on communication networks for electric system automation," *Comput. Netw.*, vol. 50, no. 7, pp. 877–897, May 2006.

[3] A. Boukerche, Horacio A. B. F. Oliveira, Eduardo F. Nakamura, Antonio A. F. Loureiro, "Secure Localization Algorithms for Wireless Sensor Networks", IEEE Communications Magazine, Security In Mobile Ad Hoc And Sensor Networks, pp: 96 –101, April 2008.

[4] D. Djenouri And L. Khelladi, A.Nadjib Badache, "A Survey Of Security Issues In Mobile Ad Hoc And Sensor Networks", IEEE Communications Surveys & Tutorials, Vol 7, No. 4 ,Fourth Quarter 2005

[5] L. L. Bello, O. Mirabella, and A. Raucea, "Design and implementation of an educational testbed for experiencing with industrial communication networks," *IEEE Trans. Ind. Electron.*, vol. 54, no. 6, pp. 3122–3133, Dec. 2007.

[6] I. F. Akyildiz, T. Melodia, and K. Chowdhury, "A survey on wireless multimedia sensor networks," *Comput. Netw.*, vol. 51, no. 4, pp. 921–960, Mar. 2007.

[7] E. Shi and A. Perrig, "Designing Secure Sensor Networks," Wireless Commun. Mag., vol. 11, no. 6, pp. 38–43, Dec. 2004.

[8] J.Broch, D. Johnson, and D. Maltz. "The Dynamic Source Routing Protocol for Mobile Ad Hoc Networks," http://www.ietf.org/internet-drafts/draft-ietfmanet-dsr-03.txt, IETF Internet draft, Oct. 1999, work in progress.

[9] D. Johnson and D. Maltz, "Dynamic Source Routing in Ad Hoc Wireless Networks," T. Imielinski and H. Korth, Eds. *Mobile Computing*, Ch. 5, Kluwer, 1996.

[10] Xiaojiang Du; Hsiano-Hwa Chen; " Security in wireless sensor networks**",** Wireless Communications, IEEE, Vol: 15, Issue 4, pp: 60 –66, Aug 2008. [9] Yong Wang, Garhan Attebury, And Byrav Ramamurthy, "A Survey Of Security Issues In Wireless Sensor Networks" , IEEE Communications Surveys & Tutorials, Volume 8, No. 2, 2nd Quarter 2006.

[11] C. E. Perkins and E. M. Royer, "Ad Hoc On-demand Distance Vector Routing," *Proc. 2nd IEEE Wksp. Mobile Comp. Sys. and Apps.*, Feb. 1999, pp. 90–100. [6] C. E. Perkins, E. M. Royer, and S. R. Das, "Ad Hoc on Demand Distance Vector (AODV) Routing, http://www.ietf.org/internet-drafts/draft-ietfmanet-aodv-06.txt, IETF Internet Draft, July 2000, work in progress.

[12] D. Maltz *et al.*, "The Effects of On-demand Behavior in Routing Protocols for Multihop Wireless Ad Hoc Networks," *IEEE JSAC*, vol. 17, no. 8, Aug. 1999.

[13] Y. C. Hu and D. Johnson, "Caching Strategies in On-demand Routing Protocols for Wireless Ad Hoc Networks," *Proc. IEEE/ACM MOBICOM '00*, Aug. 2000, pp. 231–42.

[14] S. R. Anton and H. A. Sodano, "A review of power harvesting using piezoelectric materials (2003–2006)," *Smart Mater. Struct.*, vol. 16, no. 3, pp. R1–R21, Jun. 2007.

[15] L. L. Bello, O. Mirabella, and A. Raucea, "Design and implementation of an educational testbed for experiencing with industrial communication networks," *IEEE Trans. Ind. Electron.*, vol. 54, no. 6, pp. 3122–3133, Dec. 2007.

[16] Yun Zhou; Yuguang Fang; Yanchao Zhang, "Securing Wireless Sensor Networks: A Survey", IEEE Communications Surveys & Tutorials, Vol:10, Issue 3, PP: 6 – 28, Third Quarter 2008.

[17] Erdal Çayırcı, Chunming Rong, "Security in Wireless Ad Hoc and Sensor Networks", A John Wiley and Sons, Ltd, Publication, 2009.

[18] Riaz A. Shaikh, Sungyoung Lee, Young Jae Song, Yonil Zhung, "Securing Distributed Wireless Sensor Networks: Issues and Guidelines", Proceedings of the IEEE International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing (SUTC'06), 2006.

[19] E. Aivaloglou, S. Gritzalis, and C. Skianis. Trust Establishment in Ad Hoc and Sensor Networks. In J. L´opez, editor, *1st International Workshop on Critical Information Infrastructure Security, CRITIS'06*, volume 4347 of *Lectures Notes in Computer Science, LNCS*, pages 179–194, Samos, Greece, 2006. Springer.

[20] Chris Karlof, David Wagner, "Secure routing in wireless sensor networks: attacks and countermeasures", Ad Hoc Networks, Elsevier Publications, Vol.1, pp.293–315, 2003.

[21] C. Karlof and D. Wagner, "Summary of "Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures", Seminar on Theoretical Computer Science. 27.4.2005

[22] A. Perrig, J. Stankovic, and D. Wagner, "Security in wireless sensor networks," *Commun. ACM*, Special Issue: Wireless sensor networks, vol. 47, pp. 53–57, 2004.