# Security, Privacy And Accountability In Wireless Network: A Review

Chandrashekhar Azad
Birla Institute of Technology, Mesra,Ranchi(Jharkhand)

Sumit Agrawal
DAV Institute Of Engineering & Technology Medininagar, Palamu, Jharkhand

Vijay Kumar Jha
Birla Institute of Technology, Mesra,Ranchi(Jharkhand)

**Abstract:**

Due to significant advances in information and communication technology, low power circuit design efficient to carry the sensitive information through wireless communication, wireless network have attracted attention a lot in recent years. Wireless network s is being used in many applications like Business organization, health monitoring, military operations, and home automation. While in the past wireless communication was largely limited but now days its widely used, todays wireless networks are starting to offer purely wireless communication , often mobile, and even connected operations. The purpose of this paper is to examine security, accountability and privacy issues in wireless networks. The presence of global connectivity provided by wireless communications and mobile computing has changed the way humans beings interact with each other.

**Keywords:**Wireless Network, Privacy, Security, Accountability.

## 1. Introduction:

Now day's Wireless technologies have become more and more popular in our everyday live. Personal digital assistants allow us individuals to access World Wide Web more frequently e-mail, social networking, web browsing etc. Some technologies even support global positioning system (GPS) capabilities that can locate the location of the device anywhere in the world. Wireless communication technologies promise to offer even more features and functions in the next few decades. An increasing number of agencies in different areas public sectors, private sectors, and home users are using wireless technologies in their environments. Wireless communications offer many benefits such as portability and flexibility, lower installation costs, and increased productivity. Wireless technologies cover a broad range ofcapabilities like it allows users to move their laptops from place to place within their work area without theneed for wires and without losing network connectivity. Less wiring provide greater flexibility, reliability, increasedefficiency, and reduced wiring costs in communication. Communication networks, such as those enabled by Bluetooth, allow datacommunication &synchronization with network systems and application sharing between different devices. Bluetooth functionalityalso eliminates cables for printer, scanner, plotters and other peripheral device connections. Handheld devices such asPDA and mobile phones allow remote users to synchronize personal datasand provide access to network services such as Internet access.Moreover, these technologies can offer more dramatic cost savings and new capabilities to diverse applicationsranging in different areas of organization.However, risks are inherent in any wireless communication network. Some of these risks are similar to those of wirednetworks and some are new. Perhaps the most significantsource of attack in wireless communication networks is that the technologies underlying communications medium, theairwave, is open to attackers, hackers. The loss of confidentiality and integrity and the threat of denial of service (DoS) attacks are riskstypically associated with wireless communications. Unauthorized users may gain access to communication network , corrupt the organizations data, consume network bandwidth, degrade communication

networkPerformance, launches attacks that prevent authorized users from accessing the network, or use organizations Resources to launch attacks on other communication network .

In this paper section 1 describe the introduction of the paper, section 2 provide overview of wireless network, section 3 provide accountability, privacy and security in wireless network and section 4 provide conclusion of the paper.

## 2. Wireless network:

Wireless network refers to a type of computer network that is not connected through any kind of cable. It is a method by which homes; organizations, telecommunications networks and enterprise installations avoid the costly process of introducing cables for networking, or as a connection between various equipment locations. Wireless communications networks are generally implemented and administered using radio communication, this implementation takes place at the layer of the OSI model.

### 2.1 Types of Wireless Network:

1. Wireless PAN
2. Wireless LAN
3. Wireless mesh network
4. Wireless MAN
5. Wireless WAN
6. Cellular network


Figure 1: Wireless Network

### 2.2 Literature Review:

In this paper [1], author proposed a general three-tier security framework for authentication and pairwise key establishment between mobile sinks and sensor nodes. The proposed scheme, based on the polynomial pool-based key predistribution scheme substantially improved network resilience to mobile sink replication attacks compared to the single polynomial pool-based key predistribution approach.

In [2], Authors argue that new security paradigms which exploit physical layer properties of the wireless medium, such as the rapid spatial, spectral, and temporal decorrelation properties of the radio channel, can enhance confidentiality and authentication services. In this they provide a case study for how such strategies can be integrated into a broader security framework for a wireless network

In [3], this authors examine security and privacy issues in some new and emerging wireless networks. In surveying they tried to identify new security and privacy challenges as well as inadequacies of current approaches. Certain challenges arise from the unattended, intermittently connected, and possibly mobile network operation.

In this [4] authors look into two important data security issues: secure and dependable distributed data storage, and fine-grained distributed data access control for sensitive and private patient medical data. They discussed variouspractical issues that need to be taken into account while fulfilling the security and privacy requirements.

In [5] authors proposed a novel dynamic security-aware packet-scheduling algorithm, which is capable of achieving high quality of security for real time packets while making the best effort to guarantee real time requirements of those packets. The proposed algorithm can substantially improve both quality of security and real-time packet guarantee ratio under a wide range of workload characteristics.

In [6] authors propose a framework called opportunistic encryption that uses channel

opportunities (acceptable signal to noise ratio) to maximize the throughput
subject to desired security constraints. This paper presents the following:
1) mathematical models to capture the security-throughput trade-off,
2) adversary models and their effects,
3) joint optimization of encryption and modulation (single and multirate),
4) the use of Forward Error Correcting (FEC) codes to protect encrypted packets from bit errors, 5) simulation results for Rijndael cipher.
The proposed opportunistic encryption produces significant improvement in the performance compared to traditional approaches.
In [7] author provide a comprehensive discussion of security problems and current technologies in 3G and WLAN systems and introductory discussions about the security problems in interworking, the state-of-the-art solutions, and open problems.
In [8] author give study the routing security issues of MANETs, and analyze in detail one type of attack the "black hole" problem that can easily be employed against the MANETs. In this they also proposed a solution for the black hole problem for ad hoc on-demand
Distance vector routing protocol.
In [9] authors comparatively analyze the unique network-centric features and security mechanisms of various heterogeneous wireless networks that are expected to be part of OWA. Then, after defining the specific integrated network model of OWA, they proposed an integrated security platform based on the security profile concept

**3. Security in Wireless network:**

**3.1 Accountability in wireless network:**

Accountability is an important issue in computer and network systems. One of the goals of accountability is the capability to trace an even after the event occurred so that the causes can be determined. Using accountability, one can track what happens to one's banking transactions by knowing who has logged into a bank account though a user ID, by reviewing the transactions made, and by noting other details. Accountability is being answerable, that is, taking responsibility for the transactions that are performed.



Table 1: Accountability in wireless network

| S. No. | Authors | Purposed | Remarks |
|---|---|---|---|
| 1 | Yang Xiao[10] | 1. An insurable network architecture, called A-NET.<br>2. an algorithm to achieve true accountable administration | 1. accountability with a general overview<br>2. Describes and analyzes practical framework applications of accountability systems.<br>3. accountability for wireless LANs, ad hoc networks, and wireless mesh networks |
| 2 | Yang Xiao[11] | 1. A flow-net methodology was proposed for accountability<br>2. flow-net truth finding methodology, and distributed and collaborative flow net | 1. In this they applied methodology to media access control and routing layers in wireless networks.<br>2. compare the performance of flow-net with audit log files. This article presents<br>3. approach for traffic data collection that can also be used for forensics and intrusion detection purposes. |
| 3 | LOU W et | 1. proposed a novel | 1. They addresses security and |

| | | | |
|---|---|---|---|
| | al.[12] | authentication framework that achieves enhanced user privacy protection with appropriate user accountability. | privacy issues in wireless access networks.<br>2. focused on user accountability.<br>3. discussed general approaches to achieving security and privacy and their effects on user accountability. |
| 4 | Zhifeng Xiao et al.[13] | 1. developed a hierarchical definition of P-Accountability<br>2. P-Accountability to a wireless multi-hop network system | 1. Defined P-Accountability and demonstrated its use in the hierarchical network environment.<br>2. In addition, they applied P-Accountability to a wireless multi-hop network system.<br>3. Both numerical and simulation results show that proposed approach is applicable to most accountable systems and that it provides a flexible and comprehensive view of the degree of accountability. |
| 5. | Bo Fu et al.[14] | 1. proposed a quantifiable accountability in wireless networks.<br>2. Two methods to evaluate the accountable logging of a network via the users' accepted overhead (called Q-Accountable Logging by Overhead), and P-Accountable Logging. | 1. Two methods to analyze the accountability of a network via the users' accepted overhead, called Q- Accountable Logging by Overhead, and the flow-net record depth, called P-Accountable Logging, respectively.<br>Simulation results show the feasibility and effectiveness of our flow-net scheme to achieve accountability. |



### 3.2 Privacy in wireless network:

Table 2: Privacy in wireless network

| S. No. | Authors | Proposed | Remarks |
|---|---|---|---|
| 1 | Karim El Defrawy et al.[15] | PEUC-WiN: Privacy Enhancement by User Cooperation in Wireless Networks | 1. In this paper, introduced a new scheme to improve the location privacy of wireless users while minimizing network disruption.<br>2. The proposed scheme achieves its goals by exploiting the |

| | | | |
|---|---|---|---|
| | | | collaboration among users in the same coverage area of an access point in a wireless system. |
| 2 | Wenbo He et al. [16] | privacy-preserving data aggregation schemes for additive aggregation functions:<br>1. Cluster-based Private Data Aggregation (CPDA)<br>2. Slice-Mix-AggRegaTe (SMART) | 1. The goal of our work is to bridge the gap between collaborative data collection by wireless sensor networks and data privacy.<br>2. they presented simulation results of our schemes and compare their performance to a typical data aggregation scheme – TAG, where no data privacy protection is provided. Results show the efficacy and efficiency of our schemes. |
| 3 | Riaz et al.[17] | Network Level Privacy forWireless Sensor Networks | 1. This solution comprises of Identity, Route and Location (IRL) privacy algorithm and data privacy mechanism, that collectively provides protection against privacy disclosure attacks such as eavesdropping and hop-by-hop trace back attacks.<br>2. This solution additionally provides trustworthiness and reliability. |
| 4 | Ying Jian et al. [18] | propose a locationprivacy routing protocol (LPR) | 1. location-privacy routing protocol, and combine it with fake packet injection to protect the location privacy of the receiver in a sensor network.<br>2. perform extensive simulations to evaluate LPR with false packet injection based on three criteria: delivery time, protection strength, and energy cost. |
| 5 | Jianbo et al [19] | Proposed DADPP. | 1. In DADPP , all nodes within the same cluster are partitioned into many groups according to desired privacy-levels. |
| 6 | Yanfei Fan et al[20] | 1. Network Coding Based Privacy Preservation against Traffic Analysis in Multi-Hop Wireless | 2. the proposed scheme offers two significant privacy-preserving features, packet flow untraceability and message content confidentiality, for efficiently thwarting the traffic analysis attacks. |

| | | | |
|---|---|---|---|
| | | Networks | 3. Moreover, the proposed scheme keeps the random coding feature, and each sink can recover the source packets by inverting the GEVs with a very high probability. |
| 6 | Mohamed et al [21] | 1. A Cloud-Based Scheme for Protecting Source-Location Privacy against Hotspot-Locating Attack in Wireless Sensor Networks | 1. Proposed scheme can provide a strong protection against Hotspot- Locating attack with much less energy cost comparing to global-adversary-based schemes. |
| 7 | Zhiguo et al. [22] | 1. propose a novel privacy preserving scheme based on network coding called Priv-Code to ounter against traffic analysis attacks for wireless communications. | 1. Priv-Code is able to provide strong privacy protection for wireless networks as the mix system because of its intrinsic mixing feature, and moreover, it can achieve better network performance owing to the advantage of network coding. |



### 3.3 Wireless security

Wireless security is the prevention of unauthorized access to computers using wireless networks. The most common types of wireless security are Wired Equivalent Privacy (WEP) and Wi-Fi Protected Access (WPA). WEP is a notoriously weak security standard. The password it uses can often be cracked in a few minutes with a basic laptop computer and widely available software tools. WEP is an old IEEE 802.11 standard from 1999 which was outdated in 2003 by WPA or Wi-Fi Protected Access. WPA was a quick alternative to improve security over WEP. The current standard is WPA2; some hardware cannot support WPA2 without firmware upgrade or replacement. WPA2 uses an encryption device which encrypts the network with a 256 bit key; the longer key length improves security over WEP.

**Security Goals are:**

1. Authentication
2. *Confidentiality*
3. *Integrity*
4. Data Freshness
5. Self Organization
6. Availability
7. Accessibility
8. Flexibility
9. Scalability
10. Secure Localization
11. Time Synchronization

**Security Threats:**

1. Traffic Analysis
2. Passive Eavesdropping
3. Active Eavesdropping
4. Unauthorized Access
5. Man-In-The-Middle Attack
6. Session High – Jacking
7. Replay

8. Denial of Service (DoS)
9. Interruption
10. Modification
11. Interception
12. Fabrication
13. Spoofing
14. Sniffing

Table 3: Wireless Network Security

| S. No. | Authors | Purposed | Remarks |
|---|---|---|---|
| 1 | Q.I. Ali S et al.[23] | WIDS | a new embedded wireless intrusion detection system (WIDS) is designed and implemented in order to protect a multi-services wireless network. The proposed WIDS must be in small size in order to be integrated in different wireless devices, low cost in order to be placed in many places and has good performance to cover the data rate of the WLAN. |
| 2 | Jie Yang et al.[24] | Detection and Localization of Multiple Spoofing Attackers in Wireless Networks | They used spatial information, a physical property associated with each node, hard to falsify, and not reliant on cryptography, as the basis for 1) detecting spoofing attacks; 2) determining the number of attackers when multiple adversaries masquerading as the same node identity; and 3) localizing multiple adversaries. We propose to use the spatial correlation of received signal strength (RSS) inherited from wireless nodes to detect the spoofing attacks. |
| 3 | Amar Rasheed et al.[25] | The Three-Tier Security Scheme in Wireless Sensor Networks with Mobile Sinks | The proposed scheme, based on the polynomial pool-based key predistribution scheme substantially improved network resilience to mobile sink replication attacks compared to the single polynomial pool-based key predistribution approach |
| 4 | K.Q. Yan et al.[26] | Hybrid Intrusion Detection System for Enhancing the Security of a Cluster-based Wireless Sensor Network | The proposed IDS is a Hybrid Intrusion Detection System (HIDS). It consists of anomaly and misuse detection module. The goal is to raise the detection rate and lower the false positive rate by the advantages of misuse detection and anomaly detection. |
| 5 | Weijia Wang et al.[27] | Security Analysis of a Dynamic Program Update Protocol for | Security Analysis of a Dynamic Program Update Protocol |

| | | | |
|---|---|---|---|
| | | Wireless Sensor Networks | |
| 6 | Mauro Conti et al.[28] | Distributed Detection of Clone Attacks in Wireless Sensor Networks | proposed a new self-healing, Randomized, Efficient, and Distributed (RED) protocol for the detection of node replication attacks, and we show that it satisfies the introduced requirements. |
| 7 | George Lapiotis et al.[29] | A Policy-based Approach to Wireless LAN Security Management | presented a hierarchically distributed policy-based system architecture and prototype implementation for WLAN security management. |
| 8 | Debao Xiao et al.[30] | Intrusion Detection based Security Architecture for Wireless Sensor Networks | proposed a security architecture for self-organizing mobile wireless sensor networks. It can prevent most of attacks based on intrusion detection. Then an analysis of each layer in our security architecture is discussed and the secure measures in the link layer and network layer are described in detail especially. |

**4. Conclusion:**

It is essential for organisations have suitable protective measures for their IT systems particularly where wireless technologies are used. Management policies and procedures of the organization should ensure that new technologies cannot be introduced without the knowledge of Information technology management. The wireless standards IEEE 802.11, although not foolproof, to do provide basic security. Implementing the best security standards with the use of wireless technologies and save your organisation from potentially costly attacks.

**References:**

1. Rasheed A., Mahapatra R. N., "The Three-Tier Security Scheme in Wireless Sensor Networks with Mobile Sinks", IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, VOL. 23, NO. 5, MAY 2012.
2. Mathur S., Reznik A., Ye C., Mukherjee R., Rahman A.,Shah Y., Trappe W. , Mandayam N., "Exploiting the physical layer for enhanced security". IEEE wireless communications , October 2010.
3. Ma D., Tsudik G.,"Security and privacy in emerging wireless networks". IEEE Wireless Communications • October 2010
4. LI M.,LOU W., "Data security and privacy in wireless body area networks". IEEE Wireless Communications ,2010.
5. Qin X., Alghamdi M., Nijim M. , Zong Z., Bellam K. , Ruan X., Manzanares A., "Improving Security of Real-Time Wireless Networks Through Packet Scheduling". IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS, VOL. 7, NO. 9, SEPTEMBER 2008
6. Haleem M. A., Mathur C. N., Chandramouli R., Subbalakshmi K.P., "Opportunistic Encryption: A Trade-Off between Security and Throughput in Wireless Networks". IEEE transactions on dependable and secure computing, VOL. 4, NO. 4, 2007.
7. Shin M., Ma J., Mishra A., Arbaugh W. A., "Wireless Network Security and Interworking"., Proceedings of the IEEE, VOL. 94, NO. 2, FEBRUARY 2006
8. Deng H., Li W., "Agrawal D. P.,Routing Security in Wireless Ad Hoc Networks"., IEEE Communications Magazine • October 2002.
9. JEONG J.,HAAS Z. J., "An integrated security framework for Open wireless networking architecture"., IEEE Wireless Communications • April 2007.

10. Yang Xiao, “Accountability for Wireless LANs,Ad Hoc Networks, and Wireless Mesh Networks”, 2008, IEEE.
11. Yang Xiao, “Flow-Net Methodology for Accountability in Wireless Networks”, 2009 IEEE.
12. LOU W., REN K., .“Security, privacy, and accountability in wireless access networks”.IEEE Wireless Communications 2009.
13. Zhifeng Xiao, Yang Xiao, “A Quantitative Study of Accountability in Wireless Multi-hop Networks”, 2010 39th International Conference on Parallel Processing, IEEE.
14. Bo Fu and Yang Xiao,"Q-Accountable: A Overhead-based Quantifiable Accountability in Wireless Networks",9th annual IEEE consumer communication and networking conference-security and content protection.,IEEE, 2012.
15. Karim El Defrawy and Claudio Soriente," PEUC-WiN: Privacy Enhancement by User Cooperation inWireless Networks", IEEE, 2006.
16. Wenbo He,Xue Liu,Hoang Nguyen, Klara Nahrstedt, Tarek Abdelzaher, "PDA: Privacy-preserving Data Aggregation in Wireless Sensor Networks",IEEE INFOCOM 2007 proceedings.
17. Riaz Ahmed Shaikh, Hassan Jameel, Brian J. d’Auriol, Sungyoung Lee,Young-Jae Song," Network Level Privacy forWireless Sensor Networks",The Fourth International Conference on Information Assurance and Security, IEEE 2008.
18. Ying Jian, Shigang Chen, Zhan Zhang, and Liang Zhang, "A Novel Scheme for Protecting Receiver’s Location Privacy in Wireless Sensor Networks", IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS, VOL. 7, NO. 10, 2008.
19. Jianbo Yao,Guangjun Wen, "Protecting Classification Privacy Data Aggregation in Wireless Sensor Networks", IEEE, 2008.
20. Yanfei Fan et al.,"Network Coding Based Privacy Preservation against Traffic Analysis in Multi-Hop Wireless Networks", IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS, VOL. 10, NO. 3, MARCH 2011.
21. Mohamed M.E.A. Mahmoud and Xuemin (Sherman) Shen, "A Cloud-Based Scheme for Protecting Source-Location Privacy against Hotspot-Locating Attack in Wireless Sensor Networks" IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, VOL. 23, NO. 10, 2012.
22. Zhiguo Wan, Kai Xing, Yunhao Liu,"Priv-Code: Preserving Privacy Against Traffic Analysis through Network Coding for Multihop Wireless Networks,"2012 Proceedings IEEE INFOCOM.
23. Q.I. Ali S. lazim,"Design and implementation of an embedded intrusion detection system for wireless applications",IET Inf. Secur., 2012, Vol. 6, Iss. 3, pp. 171–182.
24. Jie Yang, Yingying Chen, "Detection and Localization of Multiple Spoofing Attackers in Wireless Networks",IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, VOL. 24, NO. 2013
25. Amar Rasheed, Rabi N. Mahapatra, "The Three-Tier Security Scheme in Wireless Sensor Networks with Mobile Sinks",IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, VOL. 23, NO. 5, MAY 2012.
26. K.Q. Yan, s.c. Wang et al.,"Hybrid Intrusion Detection System for Enhancing the Security of a Cluster-based Wireless Sensor Network",IEEE 2010.
27. Weijia Wang, Lei Hu, and Yong Li,"Security Analysis of a Dynamic Program Update Protocol for Wireless Sensor Networks",IEEE COMMUNICATIONS LETTERS, VOL. 14, NO. 8, AUGUST 2010.
28. Mauro Conti, Roberto Di Pietro,"Distributed Detection of Clone Attacks in Wireless Sensor Networks",IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING, VOL. 8, NO. 5, SEPTEMBER/OCTOBER 2011.
29. George Lapiotis, Byungsuk Kim, Subir Das and Farooq Anjum, "A Policy-based Approach to Wireless LAN Security Management",IEEE 2007.
30. Debao Xiao , Chao Chen, Gaolin Chen, "Intrusion Detection based Security

Architecture for Wireless Sensor Networks", Proceedings of ISCIT 2005.