ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 6, June 2017

Security and Efficient Routing with Mesh Networks using PASER

Tanushree Lothe, Prof. P. B. Mali,

M. E Student, Dept. of Computer Engineering, STES's SKN College of Engineering, Pune, Maharashtra, India

Professor, Dept. of Computer Engineering, STES's SKN College of Engineering, Pune, Maharashtra, India

ABSTRACT: In an unforeseen event causing great loss need of some UAV's to surmount the destroyed network. On-demand network admittance and penetration of sized areas of network done thoroughly in WMN. Attacks on network and security in the wireless network are major challenges. Thus the diversion of path by the attacker or packet does not received by destination node further the network breaks needlessly and routing efficiency problem arises. In previous work the standards of security 802.11i/s are unguarded to routing attacks. In WMN there is need of protocols to route and to secure to make easy implementation of UAVs. Because of high overhead and strong assumption no any research approach approved this in practice. With use of the dynamic secure routing protocols attack prevention done in proposed protocol PASER (Position Aware, Secure and Efficient Routing) than the IEEE standards of security 802.11i/s which gives advantage over existing approach. Performance by PASER is similar with well-established unsecured routing protocol HWMP which are merged with the IEEE 802.11s security mechanisms.

KEYWORDS: PASER, Wireless Mesh Network, Hop to Hop to communication, GTK, SEEHR, DSR, Attack Detection, Authentication

I. Introduction

In wireless sensor network clustering of sensor nodes is one of the most useful methods because of its good scalability and the support for data aggregation. Data aggregation combines data packets from multiple sensor nodes into one data packet by removing same information. This reduces the transmission load and the total amount of data. With this, energy consumption is reduced in clustering, because the energy load is well balanced by dynamic selection of cluster heads. By changing the cluster head role among other sensor nodes dynamically in WSN, each node is expected to expend the same amount of energy over time. Nevertheless, as with usual multi-hop forwarding, a CH around a sink tends to have higher traffic than other CHs. As a result, nodes around sinks node die earlier than other nodes, even in clustered WSN. In a multiple-sink WSN, sensor nodes are divided into a few clusters. Sensor nodes within a cluster are connected with one sink, which belongs to that cluster. There are number of scenario where wireless mesh network is designed to implement an energy efficient communication between wireless sensors in the network. In wireless unmanned network sensor works data collection and transmission for wireless media like airborne mesh network, polar weather monitoring.

Wireless Mesh Networks (WMNs) are a good representative as they have the aforementioned features and they offer a physical air-to-air link for a direct communication between the UAVs. Proposed work enhance the existing work of symmetric key and asymmetric key cryptography by implementing public key infrastructure with every sensor node having paired key that is public and private key for message authentication. This system intimates the vulnerable attack detection by classification warm hole node and black hole nodes disaster relief for WSN. PASER has a more efficient and robust route discovery process than ARAN and BATMANS, and it is scalable with respect to network size and traffic load. PASER gains comparatively high performance to that of HWMPS. This combination of values (security and performance) is deemed to be necessary by the IETF Keying and Authentication for Routing Protocols (KARP) group to drive a broad deployment of a secure routing protocol. The latter mainly includes attacks on the core service of the mesh backbone, which is routing, such as the wormhole and black hole attacks, and user-related attacks, e.g., attacks on the user privacy with respect to data content, traffic flows, and location. Thus focus on the security of the routing functionality.

DOI: 10.15680/IJIRCCE.2017. 0506163

This work also emphasize on network lifetime by energy residual implementation using bellman ford approach for shortest distance communication. In advance this communication work on,

1. Node replication attacks
2. Attacks against privacy
3. Physical attacks
4. Networking jamming attack

To deal with above attack proposed system implements mechanism PASER (Position Aware Secure Routing).

II. RELATED WORK

I. Sugino referred way to reinforce the communication network against future unforeseen event causing great loss. After earthquake in Japan, in the discussion they include important focal point of effective measures in everyday life. They focused on the collision of the earthquake, the tsunami on Japans telecommunication networks, recovery efforts, action plans and RD policy towards building dependable future network infrastructure [2]. A. Abdulla, Z. Md. Fadlullah, H. Nishiyama, N. Kato, F. Ono, and R. Miura researched that from recent technology of networks which is frame of multiple UAS and ground stations, UAS-aided communications networks. The research challenge on primary principles amazing such networks, which is how energy efficiency openly maximizes (throughput per energy) in networks consisting adaptive modulation capable ground nodes. Further-more, maximizing clear energy efficiency reduced as a potential game played between the ground nodes which are multiple and authorized its stability, desirability and convergence. Collection of data is the method suggested so that the energy efficiency maximizes with a cleared restriction with basics of reduced potential game. Additionally, suggested data collection method of game-theoretic has the cost of Anarchy analysis. Extensive simulations exhibit the capacity of proposal under different environments [3].

L. Techy, C. Woolsey, and D. Schmale explored that the volume of air sampled by the UAV's maximization with having the initialization time period must be as short as possible during an individual sampling mission. Bounded curvature for minimum time paths the geometric method which is part of Dublin's well-known results it produces in steady winds the candidate time best paths. To defeat collision this phenomenon required to coordinate their movement in line with their respective paths used to produce paths for both UAV's. The described methods were tested during an aerobiological sampling experiment focusing on the plant pathogen Phytophthorainfestans [4].

L. Abusalah, A. Khokhar, and M. Guizani explained topology of dynamic network, finite battery power, finite bandwidth, routing in a MANET which are specifically difficult task compared to a conventional network due to its characteristics having uniqueness. Highly dynamic network has effective routing mechanism which is centered in the MANET research. Distinct routing protocols which are efficient have been suggested for MANET presently [5]. N. Kato, Y. Nemoto, A. Jamalipour, H. Nakayama and B. Kannhavong researched that in ad hoc networks with multi-hop, mobile nodes acts together to form a network without using any basic facilities and services such as base stations or access points. Rather, nodes which are movable forward packets with the hops and granting communication between nodes beyond wireless range of transmission. Essentially the finite ability of the wireless medium with wireless transmission effects like attenuation, interference and multipath propagation, the movement of nodes merge to design important instigation in wireless ad-hoc network for routing protocols operation [6].

M. Sbeiti and C. Wietfeld explored that WMNs has research guides abundance of protocol proposals. Routing part is addressed in existing implementations, but the security aspects not yet improved because of high overhead and strong assumptions. Issues in security in WMN contented with well-known unsecured routing protocols such as HWMP, OLSR or BATMAN could be merged with the standards of security IEEE802.11i/s [7]. M. Sbeiti, J. Pojda, and C. Wietfeld explained, explored that because of high performance and low cost the WMN are attracted for ever-present access in emergency and rescue operations. Here, proposed secured protocol PASER has been designed in critical environments to address the security in mesh networks. Ad-hoc routes which are reliable are forced between nodes in network and to battle unsubstantiated nodes of moving the route look-up process is done. Its light-weight symmetric authentication scheme is notable [8]. K. Sanzgiri, D. La Flamme, B. Dahill, B. Levine, C. Shields, and E. Belding-Royer says in ad hoc routing provision of efficient mechanism sending paths in dynamic networks without considering security aspects gives problem. Thus in an ad hoc network more attacks used to move the routing. Therefore specifically this threat shows their effects on ad hoc on-demand distance vector and DSR [9].

III. PROPOSED SYSTEM

A. System Architecture

The security in WMN is necessary having security at greater extent. The security is provided in the previous work with standards of security 802.11i/s. But these are unnecessarily not effective. These security standards need to use with effective routing protocols. Now in this work, the prevention of attacks routing overcome with this PASER using security mechanism like with the SEEHR Secure Energy Efficient Hierarchical Routing protocol and routing mechanism using DSR(Dynamic Source Routing). Thus these standards are used combined with security standards to prevent attacks from forgery. With the help of SEEHR, if the path between source and destination is busy or attacked then the offline path is created for packet transmission. Thus the energy of node to send packet is reduced. Modules used in this system explained below.

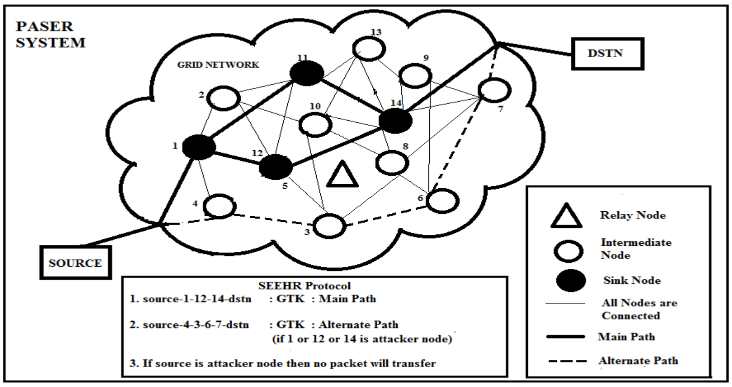

PASER
SYSTEM
GRID NETWORK
DSTN
SOURCE
1
2
3
4
5
6
7
8
9
10
11
12
13
14
SEEHR Protocol
1. source-1-12-14-dstn : GTK : Main Path
2. source-4-3-6-7-dstn : GTK : Alternate Path (if 1 or 12 or 14 is attacker node)
3. If source is attacker node then no packet will transfer
Relay Node
Intermediate Node
Sink Node
All Nodes are Connected
Main Path
Alternate Path

Fig.1 System Architecture of Proposed System

1) WSN formation with Mesh

In this module WMN is designed with network nodes interconnected to each others. It is good candidate network for air to air network for direct communication.

2) Route Discovery

Wireless network used for packet transmission from multiple sources to respective destinations. Here in this network communication bellman ford equation calculates shortest path network link. For network data downlink and uplink created. DSDV algorithm is used for shortest path. AODV is ad-hoc on demand distance vector routing protocol used for the routing of packet in network with the routing table stored at each node. It is store and forward concept.

3) Key Cryptography

The network nodes are assigned with secret key for secure wireless packet transmission. Random key generation algorithm is for producing network access keys. Asymmetric key Encryption is used for the key cryptography.

4) Key Authentication

At the time of packet transmission network nodes assumed to be verified for their assigned key if network access computed node is authorized to send packet across the network. GTK that is group transient key is used for secure communication. Node not having GTK acts as a attacker node in network default. SHA-256 algorithm for the key generation which gives hash values that are unique thus here also security of message is prevented.

B. Mathematical Model

1) Shortest Path Mechanism

Input is given as:

A graph with vectors and edges,

$$G = (V, E)$$

- The edges can be directed or not
- We grant negative edge weights

Output:

Two nodes A and B that reduces the total weight or cost length and path is created between them. Sometimes, we compute all-pair shortest paths. While sometimes, calculate shortest paths from A to all other nodes.

2) Destination Sequenced Distance Vector

Bellman Ford equation part of DSDV where each node has routing table and it is maintained which creates path which is shortest to respective destination node in the network. Multi-hops up to the destination produced. At each node to distinguish theft routes from new node and avoid from routing loops the sequence numbers are used. A new broadcast route contains,

- Destination Address
- Multi-hops for packet reception at the destination.
- Sequence number of the packet updated at each node to deliver at destination and a sequence number formed is unique to broadcast.

To maintain table consistency the routing tables updating done periodically. Each node has routing table that consists of information about destination address.

Graph:
G = {R, L}

R = set of routers,
{a, b, c, l, m, n}
L = set of links,

{(a, b), (a, l), (b, l), (b, c), (l, c), (l, m), (c, m), (c, n)}

3) DSDV Algorithm

Bellman Ford Equation given as,

$D_l(m)$ =Path cost from x to which is least then,

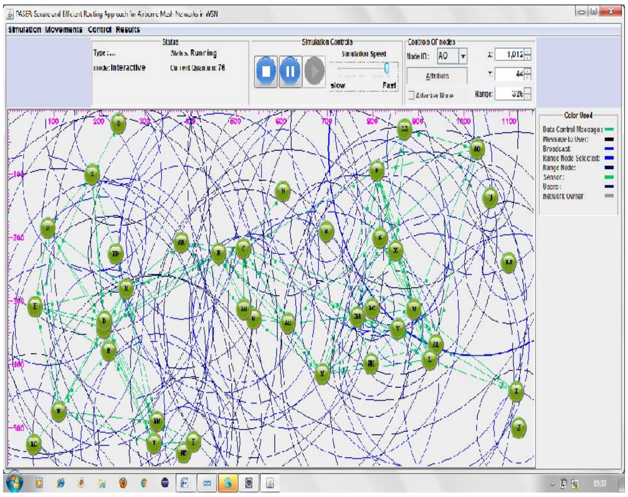
$$D_l(m) = \min (C(l, b) + D_m(m)) \qquad \ldots\ldots\ldots\ldots\ldots \quad (1)$$

Where D is Shortest Distance of X and Y coordinate and C is shortest path cost between two vectors.

4) Asymmetric Key Encryption

The encryption process where encryption and decryption done with two keys that are private and public. These different keys mathematically related gains the feasibility by cipher text decryption to get plaintext.

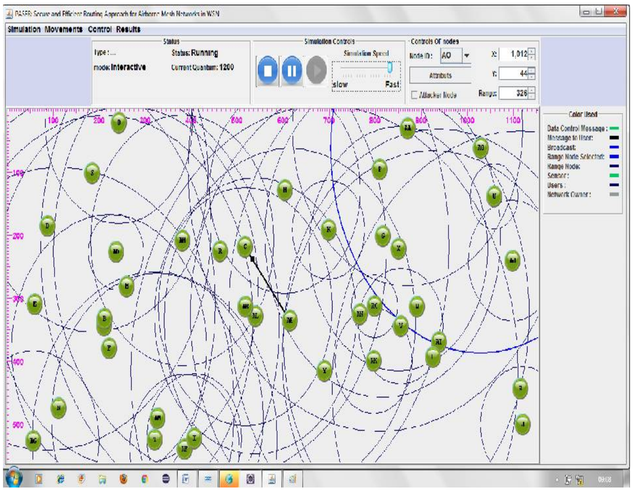
- User has public and private key. Encryption done by public key and decryption by private key.
- Public key broadcasted and private key is known to only that respective user. Hence, it is Public Key Encryption.
- It is impossible computationally in practice to find one from another. This is strength of this scheme.
- Host1 sends data to Host 2, he gets from storage public key of Host 2, data encryption by Host 2’s public key and transmits.
- Host 2 to extracts the plaintext using own private key.
- Encryption has large key length thus encryption-decryption process is slower than Symmetric Key Encryption. Computer system need to run asymmetric algorithm is higher need to take care of power of processing.



Type :...
mode: Interactive
Status: Running
Current Quantum: 76
Node ID: AO
X: 1,012
Y: 44
Range: 326

Data Control Message: 🟩
Message to User: ■
Broadcast: 🟦
Range Node Selected: 🟦
Range Node: ■
Sensor: 🟩
Users: ■
Network Owner: ▨

Fig.2 Node creation in simulation area



Type :...
mode: Interactive
Status: Running
Current Quantum: 1200
Node ID: AO
X: 1,012
Y: 44
Range: 326

Data Control Message: 🟩
Message to User: ■
Broadcast: 🟦
Range Node Selected: 🟦
Range Node: ■
Sensor: 🟩
Users: ■
Network Owner: ▨

Fig.3 Packet sent between source-destination (shortest path)

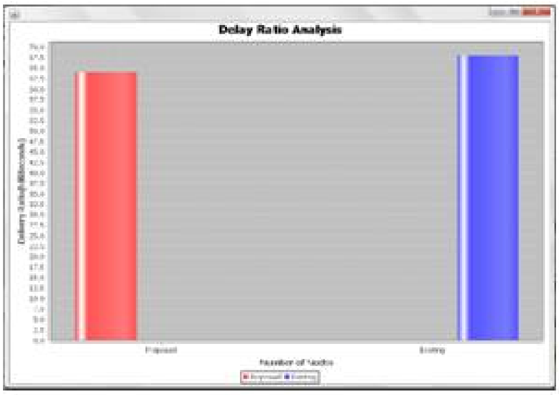


Fig.4 Packet delay ratio

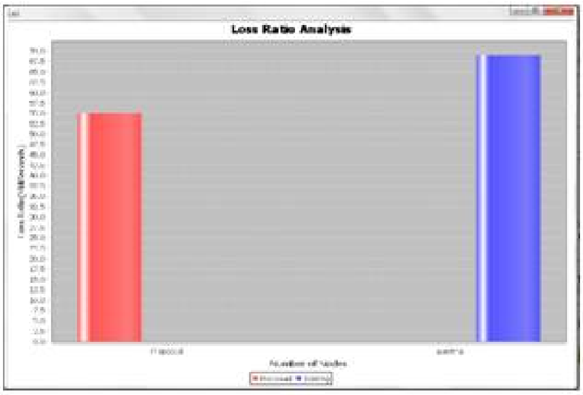


Fig.5 Packet Loss Ratio

IV. Simulation Results

The simulation is done in such a way that it runs in specified simulation area with any number of nodes. Thus in Fig 2, nodes are created with given number manually. When nodes are created, the encrypted key is assigned with every node which is unique and it is done with SHA-256 algorithm. The Key Generation, Key Authentication and Key Cryptography also get achieved using SHA-256 algorithm and Asymmetric Key Encryption. After initializing nodes all nodes get configured and having unique key called it as Group Transient Key (GTK). Then in Fig.3 the source and destination it selected and appropriate shortest path find with the Destination Sequence Distance Vector Algorithm (DSDV). To route the path DSR used and to maintain route table Ad-Hoc on Demand Distance Vector (AODV) routing protocol is used. At network layer SEEHR protocol used for security of nodes. The hierarchical structure helps to improve energy efficiency in routing. The message is encoded and decoded for the message security purpose. All these actions are done in the ECLIPSE simulation software. The Packet delay ratio(Fig.4), Packet loss ratio (Fig.5), and Throughput Analysis Ratio (Fig.6), are compared between proposed system (red bar graph) and the existing system (blue bar graph).Packet delay, Packet loss and Throughput get improved and maximize than the existing system.

V. Conclusion and Future Work

Thus with the help of above graphs it showed that parameters used for proposed approach like throughput ratio, packet delay ratio and packet loss ratio are better and improved than the existing approach. Proposed approach that is PASER protocol improves the drawbacks of existing system such that attacks vulnerability with 802.11i/s. The node security issues are overcome using SEEHR. To maintain the routing table security the AODV protocol used. Furthermore, the authentication while transmitting packet is achieved using GTK, Asymmetric Encryption and SHA-256 algorithm. Fig.7 attack detection also be done here, assigning attacker node manually. Therefore, in simple way we can conclude that security and routing efficiency get improved than the previous approach. Proposed work can be enhanced by real time implementation with airborne vehicular network to deal traffic management and cooperative communication to overcome collision in network traffics.

DOI: 10.15680/IJIRCCE.2017. 0506163

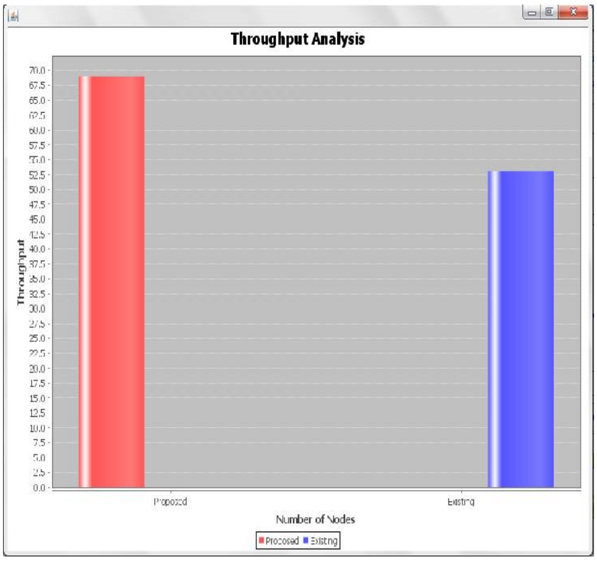
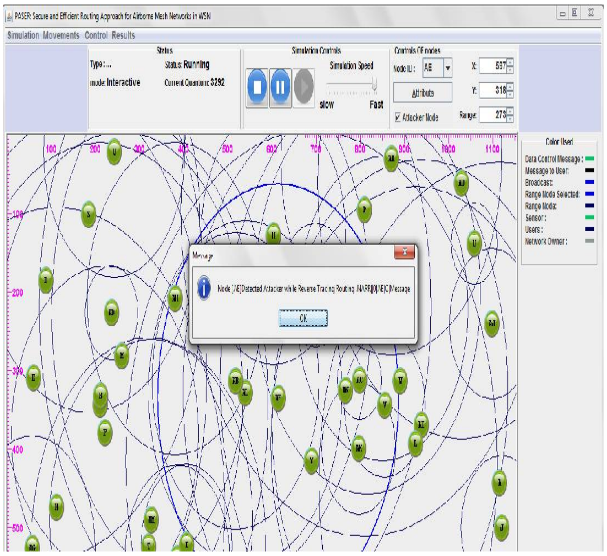


Fig.6 Throughput Analysis Ratio



Type : ...
mode: Interactive
Status: Running
Current Quantum: 3292
Node ID : AE
X: 597
Y: 318
Range: 273
☑ Attacker Node

Node [AE]Detected Attacker while Reverse Tracing Routing .NARR||0|AE|C|Message

Fig.7 Detection of attacker node

REFERENCES

1. M. Sbeiti, N. Goddemeier,D. Behnke, and C. Wietfeld, "PASER: Secure and Efficient Routing Approach for Airborne Mesh Networks", IEEE Transaction on Wireless Communication, vol. 15, no. 3 March 2016.
2. I. Sugino, "Disaster recovery and the RD policy in Japans telecommunication networks", in Proc. Opt. Fiber Commun. Conf. Expo. /Nat. Fiber Optic Eng. Conf. (OFC/OFOEC), 2012.
3. A. Abdulla, Z. Md. Fadlullah, H. Nishiyama, N. Kato, F. Ono, and R. Miura ,"Toward Fair Maximization of Energy Efficiency in Multiple UAS-Aided Networks: A Game-Theoretic Methodology", IEEE Transactions On Wireless Commu., Volume 14, number 1, Jan 2015.
4. L. Techy, C. Woolsey, and D. Schmale, "Path planning for efficient UAV coordination in aerobiological sampling missions", in Proc. IEEE Decision Control (CDC), 2008, pp. 28142819.
5. L. Abusalah, A. Khokhar, and M. Guizani, "A survey of secure mobile ad-hoc routing protocols", IEEE Commun. Surveys Tuts. vol. 10, no. 4, pp. 78–93, Jan. 2008.
6. N. Kato, Y. Nemoto, A. Jamalipour, H. Nakayama and B. Kannhavong, "A survey of routing attacks in mobile ad hoc networks", IEEE Wireless Commun., vol. 14, no. 5, pp. 8591, Oct. 2007.
7. M. Sbeiti and C. Wietfeld, "One stone two birds: on the security and routing in wireless mesh networks", in Proc. IEEE Wireless Commun. Netw. Conf. (WCNC), 2014, pp. 24862491.
8. M. Sbeiti, J. Pojda, and C. Wietfeld, "Performance evaluation of PASER An efficient secure route discovery approach for wireless mesh networks", in Proc. IEEE Int. Symp. Pers. Indoor Mobile Radio Commun. (PIMRC), 2012, pp. 745751
9. K. Sanzgiri, D. La Flamme, B. Dahill, B. Levine, C. Shields, and E. Belding-Royer, "Authenticated routing for ad hoc networks", IEEE J.Sel. Areas Commun. vol. 23, no. 3, pp. 598610, Mar. 2005.
10. S. Zhao, R. Kent, and A. Aggarwal, "A key management and secure routing integrated framework for mobile ad-hoc networks", Ad Hoc Netw., vol. 11, no. 3, pp. 1046–1061, 2013.
11. Hassen Redwan and Ki-Hyung Kim , "Survey of Security Requirements, Attacks and Network Integration in Wireless Mesh Networks", Japan-China Joint Workshop on Frontier of Computer Science and Technology 2008.
12. Rupinder Kaur and Parminder Singh, "REVIEW OF BLACK HOLE AND GREY HOLE ATTACK", The International Journal of Multimedia & Its Applications (IJMA) Volume.6, Number.6, Dec.r 2014.

BIOGRAPHY

Tanushree Arvind Lothe is a Student in the Computer Engineering Department (Computer Networks), STES's Smt. Kashibai Navale College of Engineering, Savitribai Phule Pune University, Pune, Maharashtra, India. She received Bachelor of Electronics and Telecommunication Engineering (BE) degree in 2014 from NDMVP COE, Nashik, Maharashtra, India. Her research interests are Computer Networks (wireless networks) and Network Security.