International Journal of Engineering and Advanced Technology (IJEAT)
ISSN: 2249-8958 (Online), Volume-9 Issue-2, December, 2019

A Secured and Scalable Battle-Field Surveillance using WSN Multicasting

G. Raja Vikram, K. Shahu Chatrapati, A. V. N. Krishna

Abstract*—Real-time Battle-field surveillance using Wireless Sensor Network (WSN) is a challenging task. It demands periodic sensing, run-time decision making, and fast signal processing and high data precision. WSN for battle-field monitoring is a collection of in-expensive sensor devices capable of sensing sound and signals generated by objects. An Efficient utilization of limited resources is need of the hour in these applications. Sensor nodes must be highly dynamic in sensing and sending accurate data securely to the control centre. In this paper, The authors propose a secured and scalable mechanism to sense war field and report any intruder movement with accuracy. The Proposed approach performs better in terms of network lifetime, security and accuracy.

Index Terms*—Wireless Sensor Network (WSN), Battle-field Surveillance, WSN Applications, WSN Multicasting, WSN Coverage.

I. INTRODUCTION

Increasing popularity of Wireless sensor networks has led to its application in wide range of monitoring applications. The Ability to deploy tiny, yet powerful sensor nodes without any typical underlying setup makes them suitable for applications like Battle-field surveillance, Large Structure Monitoring, Industrial Monitoring and Health monitoring. WSNs emerged as an effective way to perform battle-field activities like intruder detection, activity monitoring and logistics in un-known terrain. In comparison with traditional networks, they offer benefits such as low network establishment effort, self-healing power and fault tolerance.

Sensor nodes are self-organizing, tiny members capable of sensing varied physical phenomenon like sound, temperature, pressure and light. Generally, in war-field applications sensors are deployed randomly and nodes are expected to organize themselves to form a multi-hop communication network. These nodes should track intruder movement, firing noise or any signals received by intruder. The Sensed data is then aggregated to reach near-by control center. This will allow early detection of intruder and in turn reduce the causalities in war field.

Revised Manuscript Received on December 30, 2019.
* Correspondence Author
G. Raja Vikram*, Assistant Professor, Vignan Institute of Technology & Science, Hyderabad (Telangana) India.
K. Shahu Chatrapati, Professor and Head, Department of Computer Science and Engineering, J.N.T.U.H College of Engineering, Manthani (Telangana) India.
A. V. N. Krishna, Professor, Department of Computer Science and Engineering, CHRIST (Deemed to be University), Bangalore (Karnataka) India.

Fig.1. Sensors randomly Deployment in Battle-filed

Fig.1 shows random deployment of sensor nodes in the tracking area. After sensing the parameter it will be communicated to a nearest control center. These control centres acts as cluster heads and equipped with additional computational and storage resources compared with normal nodes. The Local Control Centres (LCC) will aggregate received data and sends accurate results to the Base station (BS). The Base Station is well connected with external world through wired or wireless internet facility.

The Rest of this paper is organized as follows. Section 2 focus on various existing applications of WSN in battle-filed surveillance. In section 3, our approach is explained. Section 4 illustrates the experimental setup and simulation results. Finally section 5 concludes the paper.

II. APPLICATIONS OF WSN

WSNs are used various domains like military, environmental, health and home applications. They were primarily designed to applications for intruder detection and tracking, target identification, traffic monitoring, Warfield damage assessment and logistics support. Various applications are designed to perform all these tasks as shown in Fig.2. In this section, We give a brief overview of existing applications on WSN.

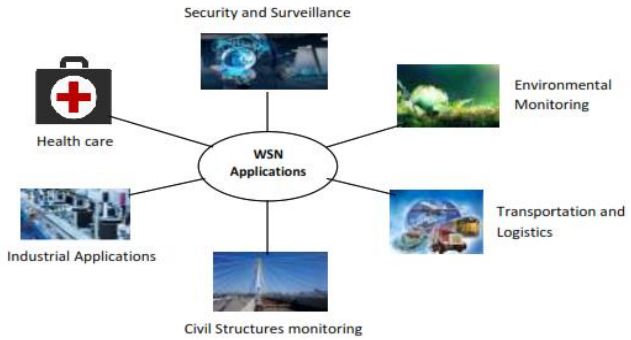


Fig.2. Applications of Wireless Sensor Networks

A. Health Applications

Various prototypes were proposed to demonstrate the application of WSN in health care domain. In this section few such prototypes are highlighted.

Sleepsafe

Based on survey, Sudden Infant Death Syndrome (SIDS) has caused unexplained deaths of infants of below one year age. An infant sleeping on stomach is most likely a victim of SIDS. Statisticsshowing approximately 2,500 SIDS deaths per year in US.

Sleep Safe prototype was primarily designed to track the sleeping position of infant and to alert parents or guardian if infant is detected to be laying on his/her stomach. The Possible positions identified by this system are- back, side and stomach. It works as follows. A Shimmer mote is seamlessly integrated into the fabric on the chest, capable of detecting whether position is anti-parallel, perpendicular or parallel to the gravity force. Another sensor is attached to a laptop, which runs a Java program responsible to check received infant's position and sends alert when infant is sleeping on stomach. To reduce proxy alerts, Java program calculates the aggregate of sensing window of previous positions.

Patient Monitoring System

It is a prudent framework which will screen different patients' wellbeing parameters in the meantime and may viably convey the information to a patient recognition framework wherever its hang on for good. Current antiquated wellbeing recognition is accomplished by singular PCs snared to each patient's bed. The various parameters that square measure observed square measure drive per unit territory, temperature, ECG, and EEG. Our examination researches the capability of WSN to confidence completely, remotely gather, send and strategy these different parameters of numerous patients in the meantime, in time of time. This is accomplished by recognizing each patient's monitored parameter utilizing a particular ID and utilizing a period programming subject all through data transmission. The framework conjointly alarms the specialist/medical caretaker of some measured value cross edge limits.

B. Environmental Applications

MAX

MAX could be a framework for human-driven pursuit of the physical world. MAX grants people to look and find physical articles when they are required. . MAX was outlined with the objectives of protection, conservative inquiry of a named question, and human-driven task. MAX utilizes a hierarchic plan that needs questions be marked, sub-stations as points of interest, and base-station PCs to discover the thing. Labels on items will be set apart as individual or open that is accessible by the general open or proprietor exclusively. MAX is expected for low vitality and negligible defer questions.

Detecting Floods

ALERT system deployed in US is equipped with sensors for measuring the downfall and weather sensors. This system provides continuous data based on the real-time environment and alerts for floods.

C. Military Applications

Early Attack Reaction Sensing Element (EARS)

Its a first of its kind sound sensing system that detects gunshot and informs the army personnel through audio and visuals. This system was designed to assist a soldier to instantly receive alerts on enemy war place.

Pinptr

Pinptr is a shooter spotting system used to recognize impacts and waves from a gunshot. A Dense deployment of sensor nodes will allow to track the impact of gunshot.

Omnibird

Omnibird is an unmanned Combat Air Vehicle (UCAV) with motion picture sensor used in day and night taking care of activities. It is equipped with an infrared sensor, and a lightweight picture taking sensor unit miniaturized with features like zoom, tilt. This setup will guide UCAV movement based on flight deck crew activity.

Acoustic Threatening Sound Recognition System (ATRS)

In Warfare to detect and counter threaten sounds we need a multi-level system. ATRS system is designed to work at various levels namely, at Base level, Cluster head level and at sensor node level to classify threatening sounds supported by processing task to collaboratively identify the targets, and distinguish proxy alarms.

D. Home Applications

Household Power Monitoring System

This system was designed to observe electrical parameters like voltage, power usage of electrical home appliances. It has a sensing unit to monitor the regular power usage in terms of an individual appliance. This allows the customer to know the per device power consumption which results in better power management.

Smart Home Vacuum (SHV) system

A Robotic Vacuum System may not completely clean few areas like stairs, beneath furniture etc.. Smart Home Vacuum (SHV) system is designed to clear all the problems with a robotic system. To enable this, SHV is embedded with Element Sensing Node (ESN) and Central Intelligent Management System (CIMS). Sensing nodes are deployed as clusters and a cluster head is selected to lead each one. The Sensed data is first send to CH, which in turn propagates the aggregated data to CIMS.

WSNs have a wide range of application areas. Especially in the context of battlefield surveillance many more applications may de designed to provide secured and scalable communication. This allows military to monitor the enemy activity in a remote location and act accordingly.

III. RELATED WORKS

In Battle-field surveillance systems energy efficiency and security plays an important role. The Work related to monitoring war-field to detect moving objects is done by several papers. The Most common approach is to cluster the sensor nodes into groups each headed by a head and apply node scheduling to reduce overall energy consumption.

In Bokareva(2006), work related to target object tracking and detection is discussed. It explained the benefits of using WSN for battle-field monitoring. One of the earliest approaches of using WSN for War-field surveillance can be seen in Wang(2003). In Gu(2005), the advantages and trade-offs of using WSN for monitoring is elaborated. In this paper, authors proposed a light-weight multi-modal detection algorithm for micro sensors. They have applied simple threshold based fusion algorithms for object detection. Both the approaches discussed in Wang(2003) and Gu(2005) have a limitation of not accounting for noise and interference.

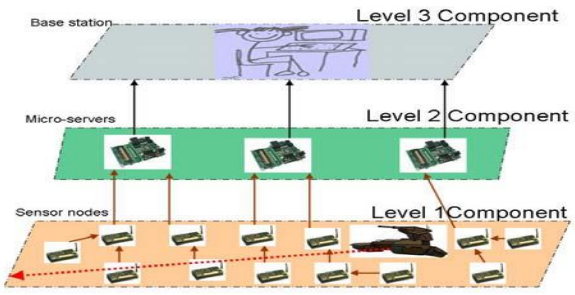
A Machine-learning algorithms based approach for vehicle tracking was proposed in Duarte(2004), where object detection algorithms like K-nearest neighbour and support vector machine classifier. The major limitation of this scheme is performing resource intensive tasks at the local node level which affects energy conservation. In Ledeczi(2005) and He(2004) , a sniper localization system were designed. These systems used acoustic signal processing and triangulation, and they used specially designed hardware for acoustic processing and object identification. Because of cost-effectiveness and resource-intensive operations they were not suitable for WSN environment. In Pattem(2003), a framework to analyze target tracking quality and energy consumption for various strategies was developed.

Node Scheduling is very important in conserving energy for WSN. When a given sensing area is covered by one or more groups of nodes, it is preferable to put few nodes in sleep state to save energy. The Active nodes are selected in such a way that the total area is covered. A review on Area coverage and connectivity for optimal performance is presented in Chaitanya(2015). The Random Back off Sleep Protocol (RBSP) was proposed in More(2014) , which decides the sleep schedule of group of nodes based on residual energy. This approach was improved by taking failed active nodes into consideration, leading to an extended network lifetime of 10.2% as explained in Chaitanya(2016).

IV. A SECURED AND SCALABLE APPROACH FOR BATTLE-FIELD MONITORING

WSN is best suited for battle-field object tracking and detection. They may be deployed in unknown terrain and needs to act reliably irrespective of ground conditions. For this reason, WSN protocols or algorithms need to address the following issues.

1. Self-Configuration
2. Extended Network Lifetime
3. Security



4. Robustness

Fig.3. Node deployment structure

Sensor nodes are randomly distributed over a given area without any proper infrastructural setup as shown in Figure 3. . The Nodes themselves should configure as a network and start communication with the Remote Base Station.

Methodology of Proposed Scheme

A. Node Scheduling

In a randomly deployed sensor network, more than one node may be covering any given area. If all the nodes sense simultaneously in a given region, the data will be redundant and it results in reduced network lifetime. To avoid this problem node scheduling is employed. According to node scheduling, nodes can be classified into two types: Active and Sleeping nodes. Only few sufficient nodes will be active at any given instance to cover the complete region. The Remaining nodes will be in sleep state. After a given time interval, the sleeping nodes probes active ones by sending HELLO packet. The Active nodes based on their residual energy will determine the Sleep Duration of inactive nodes and communicates it to them. Thus the role of Active nodes is distributed to improve the effective network lifetime. The Node Scheduling steps are given below:

Step 1: Nodes are randomly deployed in the required region.

Step 2: Nodes are classified into Active, Sleeping based on the residual energy and coverage area. If more than one node is in covering area, the highest residual energy node initially becomes active and all other nodes will become sleeping nodes.

Step 3: The Sleeping node probes active node after an interval by sending HELLO packet.

Step 4: The Active node on receiving HELLO packet calculates the sleep duration based on its residual energy and communicates it to sleep node.

Step 5: After the end of Sleep Duration the Sleeping node will become active and the active node goes to sleeping state.

In this way the nodes are scheduled to cover the given region in a energy efficient manner. The results have proven that, this approach improves overall network lifetime and reliability of network.

B. ECC Based Secured Group Key Generation

Once the node deployment process is completed, nodes are partitioned into unequal clusters based on distance from the Base station as explained in Rajavikram(2017). This will help in avoiding hot-spot problem. Node scheduling, as explained in previous section will further contributes in energy efficiency. The active nodes in a given region will react if an intruder enters into its coverage. It will send an alarming message to its cluster head in a secured way. To ensure secured communication, an ECC based multicast communication model is employed. A Binary tree is constructed for each cluster, rooted from cluster head. A Tree Vector (TV) is constructed storing the level-wise path from root to leaf nodes.

In this approach, a secured group key is generated in a contributory fashion and distributed among all the members. The Group Key generation process is explained below:

Algorithm for ECC based Group Key Calculation

a. For all the leaf nodes private and public keys are calculated as

Private Key Pr_i^h = Secret random value known only to node

Public Key $Pb_i^h = Pr_i^h \cdot G$

b. For all the intermediate nodes private and public keys are calculated as

Private Key $Pr_i^h = Pr_i^{2i} \cdot Pb_i^{2i+1}$

Public Key $Pb_i^h = Pr_i^h \cdot G$

c. For root node private key is calculated as

Private Key $Pr_i^h = Pr_i^{2i} \cdot Pb_i^{2i+1}$

Group Key $G_k^h = Pr_i^h$

where Pr_i^h, Pb_i^h are the private and public keys of a node i at a height h in binary tree.

Post group key distribution, each node upon sensing an intruder will send a alarming message encrypted using group key to all cluster head. Cluster Head in turn will forward this message so as to reach all the other cluster heads and the base station.

V. EXPERIMENTAL RESULTS AND ANALYSIS

We have simulated our approach using Java. In this simulation, 50 sensor nodes are randomly deployed in a region of length 500x500m. Each sensor node is equipped with an initial energy of 100J. The Coverage radius of a node is taken as 10m as shown in Fig.4. After the initial deployment, nodes are clustered based on the distance from the base station. The farther the cluster from the base station, the more its size would be. The Cluster length is varied such that clusters near BS will be of small in size compared with distant ones. Thus unequal clustering helps in avoiding hot-spot problem. When an intruder enters into sensing region, the nearest node will identify his movement. It will quickly transfer an ALARM packet to its cluster head. This message will propagate through the binary tree constructed to reach the cluster head encrypted using the group key. The CH upon receiving the alarm message will forward it through the optimal path constructed to reach BS.

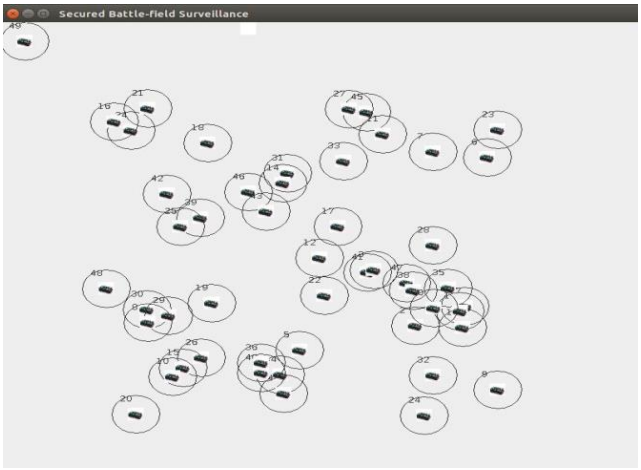


Fig.4. Simulation environment of case study

A. Security Analysis

The Major strength of ECC based approaches is the difficulty to solve discrete logarithm problem defined over an elliptic curve. Given two points P and Q on curve, it is difficult to determine a scalar value n such that P=n.Q, where "." is a scalar multiplication defined over the elliptic curve. Though the EC parameters and public keys are revealed, the eavesdropper can not determine group key due to the secret private keys.

Forward And Backward Secrecy

When a node joins or leaves a group, it sends a JOIN_REQUEST or LEAVE_REQUEST packet to the CH. Upon receiving request, the CH will initiate the new key generation process through the updated tree. This new key will be propagated securely to all the new cluster members. Thus, earlier members cannot use the past group keys to intercept and know the data under transmission.

B. Computational Complexity

ECC is a proven approach in terms of computational cost and storage requirements and well suits for energy constrained environments. For example, 4096-bit key size of the RSA gives the same level of security as the 313-bit one in ECC. As each node stores private key of itself and public keys of all other cluster members, the storage overhead is in the order of O(n). This is efficient when compared with any other public key cryptosystems. Our approach has a communication overhead of $O(\log_2 n)$, because of the binary tree optimal height. Figure 5 demonstrates the energy efficiency of proposed scheme compared with Multicast LEACH and Multicast AODV approaches. It is shown that the proposed ECC based multicasting maximizes the energy efficiency.

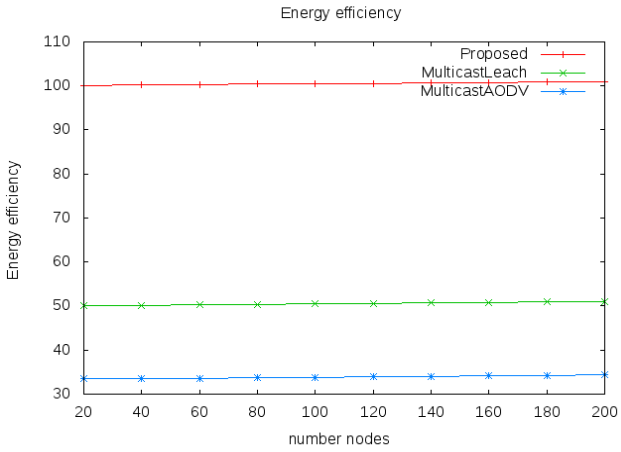


Fig.5. Comparison of Energy Efficiency

Table.1 Performance evaluation

Parameter	Other Multicast Schemes	Proposed Scheme
Approach	Distributed	Tree-based
Security	RSA or public key cryptosystem based	ECC based
Communication Overhead	O(n)	$O(\log_2 n)$
Storage Overhead	O(n)	$O(\log_2 n)$

Table 1 illustrates the performance evaluation of proposed scheme with other public key system based approaches. It is shown that, in terms of communication or computational overhead the given approach performs better.

VI. CONCLUSION

In this paper, we have explored an energy efficient and secured way of monitoring war-field. The Results demonstrated the effect of node scheduling in extending the network lifetime. It was shown that unequal cluster based group communication will further reduce the energy consumption. In Future, We plan to work with mobile sensor nodes and Base station for Battle-field surveillance. The Effect of mobility will be large on both energy consumption as well as coverage. We also plan to further extend this work, by using image sensors to track enemy activity.

REFERENCES

1. Haowen Chan, Adrian Perrig, and Dawn Song (2004), 'key distribution techniques for sensor networks',carnegie mellon university, 2004.
2. Ray, A. ; Akerberg, J. ; Gidlund, M. ; Bjorkman (2013), 'Initial Key Distribution for Industrial Wireless Sensor Networks', Industrial Technology (ICIT), 2013 IEEE International Conference doi: 10.1109/ICIT.2013.6505862 ,Page(s): 1309 – 1314.
3. The Case for Elliptic Curve Cryptography', http://www.nsa.gov/ia/industry/crypto elliptic_curve.cfm
4. Yao, A.C.-C. ; Yunlei Zhao (2013), 'Online/Offline Signatures for LowPower Devices', Information Forensics and Security, IEEE Transactions, on Volume: 8 , Issue: 2 doi:10.1109/TIFS.2012.2232653.
5. A Liu and P Ning (2008), 'Tiny ECC: A Configurable Library for Elliptic Curve Cryptography in Wireless Sensor Networks', Information Processing in Sensor Networks, IPSN '08.
6. Bokareva, Tatiana, et al. "Wireless sensor networks for battlefield surveillance." Proceedings of the land warfare conference. 2006 .
7. Q. Wang, W. Chen, R. Zheng, K. Lee,and L. Sha, "Acoustic target tracking using tiny wireless sensor devices", in Proceedings of the 2nd International Conference on Information Processing in Sensor Networks (IPSN03). 2003.
8. L. Gu, D. Jia, P. Vicaire, T. Yan, L. Luo, A. Tirumala, Q. Cao, T. He, J. A. Stankovic, Abdelzaher and B.H. Krogh , "Lightweight detection and classification for wireless sensor networks in realistic environments", in Proceedings of the 3rd international conference on Embedded networked sensor systems (SenSys '05). 2005, ACM Press: San Diego, Caligornia, USA.
9. M. F. Duarte and Y.H. Hu, "Vehicle classification in distributed sensor network". Parallel Distributed Computing, 2004. 64(7): p. 826-838.
10. A. Ledeczi, A. Nadas, P.Volgyesi, G.Balogh, B.Kusy, J. Sallai, G. Pap, S. Dora, K. Molnar, M.Maroti and G.Simon,"Countersniper system for urban warfare",ACM Transactions on Sensor Networks, 2005.1(2): p.153- 177.
11. T. He, S. Krishnamurthy, J. A. Stankovic, T. F. Abdelzaher, R.S. L. Luo, T.Yan, L. Gu, J. Hui and B.Krogh, "An Energy-efficient surveillance system using wireless sensor networks", in Proceedings of International Conference on Mobile Systems, Applications, and Services (MobiSys). 2004.
12. S. Pattem, S. Poduri, and B. Krishnamachari, "Energy-quality tradeoffs for target tracking in wireless sensor networks", in Proceedings of the 2nd International Conference on Information Processing in Sensor Networks (IPSN03).2003.
13. Chaitanya Mahamuni, KTV Reddy, Nishan Patnaik, "A Literary Study of Coverage and Connectivity in Wireless Sensor Networks for Optimal Performance" International Journal of Engineering and Management (IJERM), Volume-02, Issue-11, November 2015, (pp.28-31)
14. More, Avinash, and Vijay Raisinghani. "Random backoff sleep protocol for energy efficient coverage in wireless sensor networks." Advanced Computing, Networking and Informatics-Volume 2. Springer International Publishing, 2014. 123-131.
15. Chaitanya Vijaykumar Mahamuni, K.T.V.Reddy, Nishan Patnaik," Optimal Backoff Sleep Time based Protocol for Prolonged Network Life with Blacklisting of Failure-Prone Nodes in Wireless Sensor Networks" presented at International Conference on Innovations in information, Embedded and Communication Systems(ICIIECS 2016), Coimbatore, and included in preceding, (pp.808-813).
16. G.Raja Vikram, A.V.N.Krishna, K.Shahu Chatrapati(2017). Variable Initial Energy and Unequal Clustering (VEUC) Based Multicasting in WSN. IEEE WiSPNET 2017, International Conference, 82-86.

AUTHORS PROFILE

G. Raja Vikram is presently pursuing his Ph.D from Jawaharlal Nehru Technological UniversityHyderabad, Telangana, India. Hyderabad. He has completed his M.Tech from JNTU. He is presently working as an Assistant Professor at Vignan Institute of Technology & Science, Hyderabad. He is having 13 years of teaching experience. His research areas include Multicasting in Wireless Sensor Networks , Network Security.

Dr. K. Shahu Chatrapati is working as Professor and Head of the Department, Computer Science and Engineering department at College of Engineering, Manthani, Jawaharlal Nehru Technological University, Hyderabad, TS, India. He is having 17 years of teaching experience at undergraduate and postgraduate engineering level and guiding 8 Ph. D research scholars. He published 35 research papers in national and international journals and conferences. He organized various conferences and workshops at JNTUCEM on ethical hacking, robotics with the collaboration of IIT Kharagpur and Advances in Computing and Networking sponsored by CSI. His current research interest includes Compilers, Theory of Automata, and Distributed Computing.

Dr. Addepalli V. N. Krishna is working as Professor in Computer Science and Engineering department at CHRIST(Deemed to be University), Bangalore, India. He received Ph.D in 2010 at Department of Computer Science and engineering, Acharya Nagarjuna University, AP, India and M. Tech degree in 2001 from department of Computer Science and Engineering, Birla Institute of Technology, Mesra, Ranchi, India. He is having 25 years of teaching experience at undergraduate and postgraduate engineering level and guiding 6 Ph.D research scholars from reputed universities in India. He published 35 research papers in national and international journals and 10 research papers in national and international conferences. His current research interests includes security algorithm design in wireless sensor networks, advanced key management algorithms for computer security and protocol design for network security.