IJIRSET
International Journal of Innovative Research in
SCIENCE | ENGINEERING | TECHNOLOGY

e-ISSN: 2319-8753 | p-ISSN: 2347-6710


# INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

## IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 10, Issue 10, October 2021

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 7.569

9940 572 462 | 6381 907 438 | ijirset@gmail.com | www.ijirset.com

International Journal of Innovative Research in Science, Engineering and Technology (IJIRSET)

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 7.569|

|| Volume 10, Issue 10, October 2021 ||

| DOI:10.15680/IJIRSET.2021.1010003 |

# A Security of Wireless Sensor Networks: Past, Present, and Future

**Mohamed M. Nagi Elshibani[1], Fajria Amara Saleh Zalita[2]**

Department of Computer Science, Higher Institute for Sincie and Technology – Tarhuna[1,2]

**ABSTRACT:** Given the growing range of applications and importance of decisions based on the operations of wireless sensor networks and the increased concern of security that grows with their spread, the topic of wireless network security is one of global concern with an impending and lasting future. Its importance is obvious and demanded research in its concern.

This research concentrates on the state of security of existing wireless sensor networks and the efforts that have been made in regards to such security. The scope of this work focuses on the security concerns demonstrated from the implementations and utilization of wireless sensor networks and the efforts that have been made and proposed in regards to these concerns. Several existing analyzes are to be discussed regarding the successes and failure of wireless network security schemes. What will follow from the exposition of these analyses is a discussion of their commonalities: what they agree upon and where they disagree.

**KEYWORDS:** Security Analysis, Wireless Threats, Security Measures, Wireless Sensor Networks.

## I. INTRODUCTION

The prevalence of wireless sensor networks has grown greatly over the past two decades finding applications in many fields and industries. Identifying patterns in human behaviour, utilizing human movements, and activities via ad-hoc wireless sensor networks such as cell-phone networkshas become quite common.

Everything from traffic information to trends in localized conversation based on environmental surroundings to the sounds of traffic noise to determine road conditions are all pieces of information available through vast cell-phone networks operating as wireless sensor networks. In addition, domestic applications utilizing cellphones, many applications utilizededicated devices either adapted-in-function-for or designed-for wireless sensor network usage.

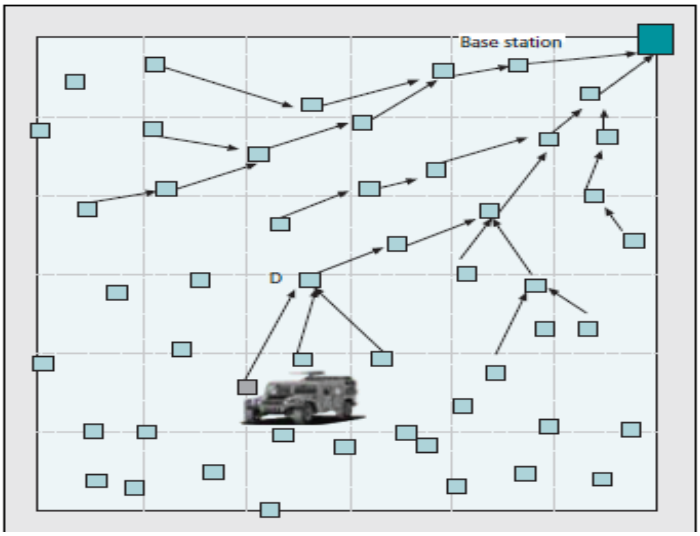


Fig.1 Traffic pattern on wireless [4]

Sensors can be utilized to detect fires or excessive heat for safety and rescue operations. They can also detect radiation levels for evaluating safety and operability in certain industrial applications. Satellites as sensors can be utilized to detect and track a widevariety of phenomena including bird flock migrations and weather patterns. Of course, there also exist

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 7.569|

|| Volume 10, Issue 10, October 2021 ||

| DOI:10.15680/IJIRSET.2021.1010003 |

long-standing applications of wireless sensor networks, such as a network of information from aerial vehicles to determine safe flight paths, adverse conditions, and other safety-critical details [1].
Given all of the potential and existing applications of wireless sensor networks ranging from simple to critical, there is a factor that should be given great consideration in determining the proper operation of wireless sensor networks like insecurity, due to the sensitive nature of some of the information utilized by certain wireless sensor networks and the bases of certain decisions made based on such information, unsecured wireless sensor networks raise risks that could potentially outweigh their uses[5]. In the work proposed, we aim to summarize and understand the state of security in wireless sensor network applications and look towards the futures of such networks in terms of the security concerns that come with them.

## II. WIRELESS SENSOR SECURITY CONCERNS

With an increase in the popularity of WSN (Wireless Sensor Network) in a wide range of applications, the issue of security has become very important. It can be argued that only a few networks need security measures. For example, a network used to read environmental information (like the sun's brightness) to observe weather patterns- does not require strong security measures [6].
But a network of sensors monitoring condition of heart must be necessarily made tamper-proof. In thiscase, it is required to link the information obtained in the first example to the network of land values, then a problem arises quickly. By twisting the information, someone can simply manipulate the value of the real estate based on changing the number of sunny days. Usually, technology outgrows its original concepts and serves as an infrastructure for some other needs. This necessitates the provision of adequate security for all types of WSNs [5].
When the cost is a fixed parameter, it becomes quite impossible to change in any other character without compromising on some other parameters. For example, multi-frequency radios and hardware security modules can be used to alleviate any problems, but these cost double the price of nodes.
When we use solutions that result in more complexity in the network, it degrades the characteristics of the network. So these need smart solutions. For example, expected lifetimeis improved with efficient sleep protocols and energy harvesting techniques, energy efficiency can be boosted. Solutions to different problems should not overstrain other components. Attacks on WSNs are listed below using a bottom-up approach and are grouped depending on the place of their occurrence using a simple taxonomy [8].

## III. RELATED NETWORK WORK

One of the man-madeartifacts that have been a great success is the Internet which has played a significant role in fundamentally changing society. With passing time, the use of the wireless internet and its basic structure has undergone various changes. All the changes have largely been driven by the interests of Internet users and the availability of the content. The existing traffic studies indicate that much of the Internet traffic is the result of content delivery and is generated by smaller infrastructure.

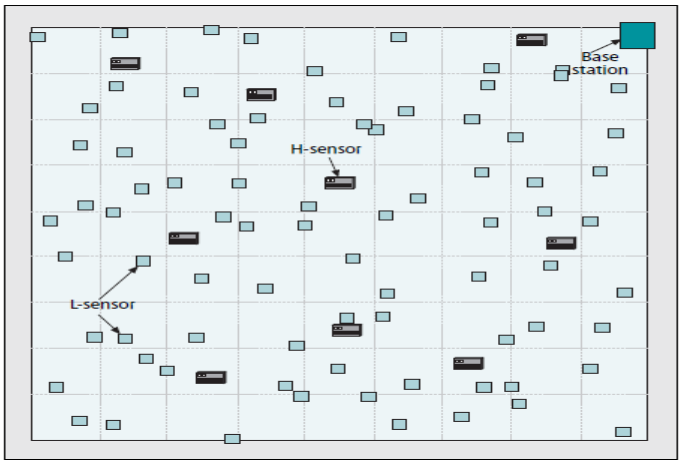


Fig.2 Traffic flow [4]

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 7.569|

|| Volume 10, Issue 10, October 2021 ||

| DOI:10.15680/IJIRSET.2021.1010003 |

Today wireless infrastructure has implemented and distributed server infrastructures for replicating the content and increase its accessibility from various locations on the Internet to deal with the rising content demand. There are three chief approaches used by these infrastructures for placing their servers.

Most of the network traffic was exchanged directly between distinct networks and residential ISPs and data centers. Big organizations like Google, which generate a huge volume of content, fail to directly connect with large network numbers and must optimize how content is generated from the network. Organizations providing Internet access to mobile or broadband users desire to optimize how traffic enters the networks because the users download much more content than what they are capable of uploading.

Traffic engineering in olden days aimed at minimization of the likelihood of bottlenecks arising within a network because of disparities between expected demand and network provisioning [5]. Changes taking place in network provisioning are usually slow-spreading over weeks or months. On the other hand, popular content triggers demand over a small period like minutes or hours.

Today, the Internet demands greater reactive network control methods that must be capable of considering content delivery. Few collaborative approaches were developed to deal with the traffic based on content delivery infrastructure. The rate of growth of network traffic is about 30% annually and is largely dominated by content delivery to the end-users.

## IV. GENERAL SECURITY THREATS

Wired networks are more prone to security threats than wired networks because of the visibility of the broadcast medium. In fact, wired networks are more harmful because of the convergence being placed in an averse surrounding which is not well guarded. Few of the security threats to the data transmitted through the network are as follows [2]:

Inclusion of hostile Code

The aforesaid is one of the most harmful attacks that can take place. These codes can be inserted into the network intersection, harming the entire network and even taking control from the opponent. A compromised network will send erroneous information about the surrounding to the authorised user or confidential information to an unauthorised user.

Intersection of the Messages[4]

Messages' providing the actual location of the nodes, with sensors help the culprit to cause harm to the insertion. to save the network, the nodes should be of small size and meticulously located. The location information, where static nodes are concerned, should be well guarded through the network's lifespan [3].

Specific Data

A rival can observe the content of the particular messages comprising of timestamps, information IDs and other details. The secrecy of the location of information is more important than the fields in the application. The particular data application does not have the important information and the lifespan of such information is short.

Feed Wrong Information

A rival can feed wrong information about the surrounding to the user. These messages also use up the limited resource of the nodes.

## V. SECURITY ANALYSIS

Confidentiality: Unauthorised user should not able to decipher the information. The rival, because of the shared network, may have access to the message being exchanged between sensor nodes. To avoid this, the messages should be efficiently crypto graphed before release.

Integrity: The ultimate user should be able to figure out any change to the message received during transference. This would help in avoiding misuse by an adversary. Message authentication codes can be used to prevent the information from leaking. The use of code as a secret key, unwelcome nodes will not be able to alter the message content.

Authentication: It is important to have message authentication in a network. It is also important for many administrative tasks. At any given point of time, a message can be hacked by a rival so the receiver should be aware that the decision-making data has come from the right source. Data authentication ensures the authenticity of the data [5].

Where two parties are involved, the data authentication can be possible through the use of a message authentication code, which is sent to the receiver by the sender. Once a message with the correct MAC is received, the receiver is ensured of its authenticity.

Access control**:** MAC can be used to prevent the in an intrusion of unauthorised nodes in the network. Unauthorised nodes will not be able to send authorised messages into the network [7].

Semantic security**:** prevents rivals from gaining access to information, even if they see numerous encryption of the message. The absence of security makes helping in traffic analysis. Using an initial value in encryption, which is used by both parties, is a common process in the symmetric block sphere to attain data symmetry.

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 7.569|

|| Volume 10, Issue 10, October 2021 ||

| DOI:10.15680/IJIRSET.2021.1010003 |

Message replay protection**:** Cryptographically safeguarded information may not be able to be deciphered by a rival but he may be able to replicate the same in the future. The method used itself needs to be safeguarded for replay attacks. Replay protection prevents the use of false and backdated information.
Freshness: Even though sensor networks use varied time calculation, the freshness of information is also important to ensure data safety and authenticity. There are two different variations of freshness: First is Weak freshness, restricted information ordering, but recent data is used. It is used by sensor measurements. Strong freshness is one, which gives detail about response-request pair, and delayed measurement is possible. It is useful for time coordination within a network [8].
Security Threats of Wireless Sensor Network
The wireless networks are usually operated over a personal or a local area and are operated by humans and they communicate with humans or with a fixed component of the system. The Wireless Sensor Networks are built with a different purpose; the communications are not based on human interaction. This is the unique challenge in securing these systems and these require reconsideration of the approaches for devising effective protection.

Wireless Threats
The most common threats are because of the very nature of communication which takes place over the wireless channel as it suffers from much vulnerability.

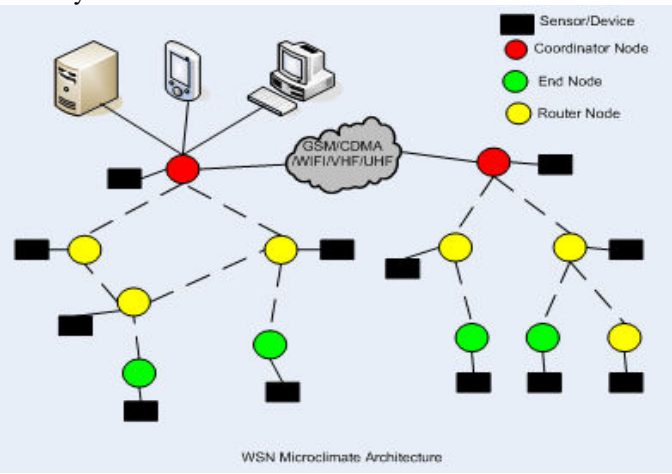


Fig.3 WSN Microclimate Architecture [4]

Eavesdropping:The easiest way is by overhearing the information transmitted by a node and then to analyze and extract sensitive information [2].
These are called *passive attacks.*
Data alteration:It is possible to collide with wireless transmission and alter the messages being transmitted. These are *active attacks.*
Identity theft: An adversary can fake a legitimate user when a legal user is not active.
Routing Threats
The simple nature of routing protocols renders them an easy target. Karlof and Wagner have classified these attacks in these categories:
Spoofed, altered and replayed routing information**:**
The data transmitted can be altered, spoofed or destroyed.
Selective forwarding: In this case, the attacked node refuses to forward all the messages received, where some messages are dropped.
Sinkhole attacks: In such an attack, the entire traffic gets attracted.
Sybil Attack**:** In this type of attack, the node appears as multiple nodes.
Wormholes**:** Here the malicious node tunnels the message from a part of the network over the non-existing link to another part of the network.
*Hello,*Flood attacks: this attack uses many protocols to broadcast "*Hello"* messages in the network. The attacker has access to the great range of transmission to send Hello messages to a large number of nodes in a wide area network.

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 7.569|

|| Volume 10, Issue 10, October 2021 ||

| DOI:10.15680/IJIRSET.2021.1010003 |

Hijacking

The adversary interferes with sensor application by obtaining control over the sensors. It is possible to execute eavesdropping and disruption attacks- from inside of the sensor network, by choosing a set of sensors to hijack. These types of attacks are most difficult to detect as they originate from the trusted nodes.

This is not the first attack model of sensor security and is unique in two ways. Firstly, this falls under the taxonomy based on the goals of adversary- and not the methods. Secondly, the overall output of the network is focused upon the certainty that an individual node is surely compromised.

Many sensor networks are not just to measure the environment; they interact with the network through actuators. If sensors are integrated with actuators, it is necessary to avoid disruption attacks on actuators too as this would be catastrophic in applications like medical or defense equipment. Even if an attacker is prevented by accessing messages or infect them, they can exhaust batteries by bogus queries. Even if the sensor and actuators can ignore these requests, nevertheless energy is spent to process these[2].

Physical Attacks

An adversary can damage hardware physically and terminate the nodes. This is also viewed as a decline in fault tolerance, which is the abilityto maintain network functionalities with node failures. Physical attacks can become a serious issue in the case of tactical communications. An adversary can physically access and destroy the sensor nodes. If such risks exist, nodes must be resilient to such attacks[1].

Potential Solutions

Bloom Filters

The chief challenge associated with name privacy concerning CON is to keep the name private making sure that there are routability and accessibility. The most obvious solution seems to be the utilization of Bloom filters for the identification of content. The architecture which has resulted comprises of three chief blocks. Firstly, it is the hierarchical bloom filter deployed in the routing table. Secondly, it is the counting bloom filter for every interface used within the PIT table. Lastly, it is the hierarchical bloom filter which is applied in the router storage [4].

Signature Privacy

The chief objective of CONs is decoupling of the content from theoriginal location and permitting the retrieval from nearest caches. Some of the CON architectures like CCNx make use of digital signatures for ensuring integrity and provenance for trusting fetched data. Even though signatures are quite strong tools for binding content with the producer, normal digital signatures might leak sensitive information regarding the signer. This becomes challenging while considering monitoring and censorship because content from a few publishers can be conveniently and easily identified from their signing key that is stated explicitly at each data packet within CCNx [4].

Confirmer Signatures

Usage of confirmer signatures is the primary approach for preventing an adversary from confirming a signature. These are irrefutable signatures in which the signer would delegate the task of verification to some third party. Thus, it is true that no signatures would be verified if interactions do not take place with the party[4].

This particular approach can be implemented easily and does not require modification of the CCNx schema; it does need a third party in the form of a confirmer and also introduces a round of communication for verification of the signature. Group signatures permit the signer to vanish among various potential signers which provide signer ambiguity. The client can now verify the generation of the signature from a group member but fails to identify the individual.

For example, a company comprising of various employees might deploy group signatures such that the signature is not traced publicly back to one user but to the company. However, such a signature is quite efficient because the signature size is not dependent on the group size. Nevertheless, the presence of a trustworthy group manager is assumed admitting revoking anonymity, distributing keys and group members within the group making it suitable in limited settings along with collaborated users [6].

Proposed Approach

However, not any of the suggested solutions protect from inside as well as outside intruders.Conversely, this can be done by intrusion detection systems. We consider that intrusion detection systems are essential for simple security mechanisms like cryptography, it is not able to provide the required security. For instance, cryptographic mechanisms offer protection against certain kinds of attacks from external nodes, but protection against malevolent inside nodes is not provided which previously have the needed cryptographic keys, so in order to detect these Byzantine nodes, intrusion detection mechanisms are essential[8].

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 7.569|

|| Volume 10, Issue 10, October 2021 ||

| DOI:10.15680/IJIRSET.2021.1010003 |

Our energy-efficient and decentralized intrusion detection system is presented in this section. First, it is observed by us that not one of the current approaches offers a comprehensive way to build an IDs, e.g., certain approaches defining their IDs making use of cluster techniques, however, it is not mentioned by them how to create a cluster and how it is going to behave.
Moreover, we consider that the restricted energy available to the sensor nodes commands the use of a categorized model for IDs, i.e., the network is allocated into clusters, wherein one node is allotted the role of the cluster head. Energy consumption is minimized by this through evading all the nodes requiring sending data to a remote base station. It is to be noted here that the clusters may be used in routing of messages, wherein every data packet is forwarded through cluster heads till it reaches the controlling center.

Cluster Formation
We make use of the cluster first protocol according to which the heads ofthe cluster are chosen after the formation of clusters. This provides the security essential to impede the external attackers to be a part of a cluster. The protocol is developed in 4 fundamental stages and an additional stage in case any irregularity is found. In the very first stage, each node computes the local maximum cluster and neighbour lists are interchanged amid neighbours. The local maximum cluster is interchanged amid neighbours and a maximum cluster is adjusted[5].
In step third, every node exchanges the updated cliques with its neighbours and its final clique is derived. In the fourth step, their final cliques are exchanged by the neighbours. In the case of detection of clique inconsistency, a fifth step is introduced where every node does conformity checking. In case of detection of a malicious neighbouring node, it will be removed from the network, and startingfrom step one the protocol restarts. The fifth step includes two stages.
Node I do conformity checking in stage A, to detect malicious nodes which sent unpredictable messages in the earlier four steps. Then node i re-computes the initial three steps of the cluster formation protocol for node j. In the case the resultant final clique is not what is received by node i from node j in the fourth step, node j is a malicious node. If the first check is not passed by node j, it implies that another common neighbour of nodes i and j sends varied messages to nodes i and j in the previous step. Hence node i can identify the malicious node k. In stage A, if the malicious node is not detected, node I enters stage B. This stage aims at detecting silence attacks in the second and third steps[5].
Another problem to be dealt with is the location of the IDs. We have to decide which nodes are to run the IDs. Based on the sets of cluster head, we use the nominal number of cluster heads cut-set smaller and makes the algorithm faster, hence more energyefficient. Then we should be ascertained that cluster nodes are not malicious and are secure.
Cluster head does this by deciding which node is energy capable to observe it. We consider that the method of using a rotating group of monitors results in aggravating the energy consumption amid the cluster's participants. At that time, every team monitors the cluster head in a round-robin schedule. In this case, the number of nodes indicating that the cluster head is malicious, then the monitoring team revokes the cluster head and one more cluster head is selected.

Rule-Based Detection
We follow a network-based approach; the intrusions get detected by monitoring messages exchanged at the sensor nodes. A set of rules are used to analyze all the messages. Da Silva et al. used an identical approach. The rules are; if a message is found violating any of these rules alarm is raised. A node where several alarms cross threshold limit, it is considered as an intruder and the cluster-head restrains it. If alarms raised by monitoring tea, are over the threshold limit, the cluster-head itself is restrained and revoked and new cluster head elected[4].
Interval rule**:** An alarm is triggered whenever the interval between consecutive messages is shorter or larger than predefined values of active event-notification task.
Retransmission Rule**:** When a message that contains information about the realization of any event is not forwarded to the controlling centres in the system, an alarm is raised [5].
Integrity rule**:** the size of message payload (potion of message containing information about the realization of any event) should be same throughout the path from sender to the receiver.
Delay Rule**:** data message retransmission must take place in the predetermined period.
Repetition Rule**:** A neighbour is allowed to transmit data message for the limited number of times only.
Radio Transmission range**:** All of data messages for the realization of a single event should originate only in one of the neighbours.
Jamming Rule**:** Number of collisions encountered by a data message should be less than expected collisions. Our IDs model can easily detect an intruder. This meets the requirements and the restriction of the WSNs and ensures that the adversarial messages get identified[4].

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 7.569|

|| Volume 10, Issue 10, October 2021 ||

| DOI:10.15680/IJIRSET.2021.1010003 |

## VI. CONCLUSION

Wireless Sensor Networks face numerous security problems because of their limited memory, less processing power and bandwidth problems. Yet, the researchers have made considerable progress in the last 5 years to apply the known security techniques to suit the embedded systems. The Network layer algorithms can detect and also stop lowerlevel attacks such as corruption and node capturing.

By using Elliptic Curve Cryptosystems, it is possible to use asymmetric cryptography. With better understanding the ways to secure routing- there is an improvement in an increase in network availability. Our study continues in the field of network layer security by using it with mobile sinks. This will help us to determine if these methods can reduce the overall stress on routing algorithms and take account of added complexities seen in mobile WSNs and still provide the same security level and detection of intruders.

## REFERENCES

[1]. Bin Yang, "Study on Security of Wireless Sensor Network Based on ZigBee Standard," *Computational Intelligence and Security, 2009. CIS '09. International Conference* , vol.2, no., pp.426,430, 11-14 Dec. 2009.

[2]. Weihong Chen; Weichu Xiao, "Model checking and analyzing the security protocol for wireless sensor networks," *Electronic and Mechanical Engineering and Information Technology (EMEIT), 2011 InternationalConference* , vol.8, no., pp.4093,4096, 12-14 Aug. 2011.

[3]. Boyle, P.; Newe, T., "Security Protocols for Use with Wireless Sensor Networks: A Survey of Security Architectures," *Wireless and Mobile Communications, 2007. ICWMC '07. Third International Conference*, vol., no., pp.54,54, 4-9 March 2007.

[4]. Xiaojiang Du; Hsiao-Hwa Chen, "Security in wireless sensor networks," Wireless *Communications*, IEEE , vol.15, no.4, pp.60,66, Aug. 2008.

[5]. El-Saadawy, M.; Shaaban, E., "Enhancing S-LEACH security for wireless sensor networks," *Electro/Information Technology (EIT), 2012 IEEE International Conference*on *Electronic/Information Technology* (*EIT*) , vol., no., pp.1,6, 6-8 May 2012.

[6]. Karapistoli, E.; Economides, A.A., "Wireless sensor network security visualization," *Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT), 2012 4th International Congress*, vol., no., pp.850,856, 3-5 Oct.2012.

[7]. Hai Liu; Xiaowen Chu; Yiu-Wing Leung; Rui Du, "Minimum-Cost Sensor Placement for Required Lifetime in Wireless Sensor-Target Surveillance Networks," *Parallel and Distributed Systems, IEEE Transactions*, vol.24, no.9, pp.1783,1796, Sept. 2013.

[8]. Kashif Kifayat, Madjid Merabti, Qi Shi, David Llewellyn-Jones, "*Handbook of Information and Communication Security* ", 2010, pp 513-552

INNO SPACE
SJIF Scientific Journal Impact Factor

Impact Factor:
7.569

doi cross ref

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर NISCAIR

# INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

## IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details