Volume 6, Issue 3, March 2016 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

# A Research Study of Wireless Network Security: A Case Study

**Sunita Saini**
Research Scholar JJT, University,
Rajasthan, India

**Dr. Yogesh Kumar Sharma**
Associate Professor JJT, University,
Rajasthan, India

***Abstract: Remote systems administration gives numerous preferences, yet it likewise combined with new security dangers and changes the association's general data security hazard profile. Despite the fact that execution of mechanical arrangements is the typical react to remote security dangers and vulnerabilities, remote security is fundamentally an administration issue. Viable administration of the dangers connected with remote innovation requires a sound and exhaustive evaluation of danger given the earth and advancement of an arrangement to alleviate recognized dangers. We show a structure to offer chiefs some assistance with understanding and evaluate the different dangers connected with the utilization of remote innovation. We additionally talk about various accessible answers for countering those dangers.***

***Keywords: wireless network, wireless security, wireless threats, signal-hiding***

## I. INTRODUCTION

Remote systems administration presents numerous points of interest Productivity enhances as a result of expanded openness to data assets. System arrangement and reconfiguration is less demanding, quicker, and less costly. In any case, remote innovation likewise makes new dangers and modifies the current data security hazard profile. For instance, since interchanges happens "through the air" utilizing radio frequencies, the danger of capture is more prominent than with wired systems. On the off chance that the message is not encoded, or scrambled with a powerless calculation, the assailant can read it, in this way trading off secrecy. Albeit remote systems administration modifies the dangers connected with different dangers to security, the general security targets continue as before as with wired systems: protecting classification, guaranteeing respectability, and keeping up accessibility of the data and data frameworks. The target of this paper is to help administrators in providing so as to settle on such choices them with an essential comprehension of the way of the different dangers connected with remote systems administration Furthermore, accessible counter measures. The prominence of remote Networks is a confirmation principally to their benefit, cost proficiency, and simplicity of incorporation with different systems and system segments. The dominant part of PCs sold to customers today come pre-furnished with all fundamental remote Systems innovation. The advantages of remote Networks include: Convenience, Mobility, Productivity, Deployment, Expandability and Cost.

Remote Network innovation, while loaded with the accommodations and points of interest depicted above has its offer of destructions. For a given systems administration circumstance, remote Networks may not be attractive for various reasons. The majority of this need to do with the intrinsic constraints of the innovation. The hindrances of utilizing a remote system are: Security, Range, Reliability, and Speed. Remote Networks show a large group of issues for system supervisors. Unapproved accesses focuses, showed SSIDs, obscure stations, and satirize MAC locations are only a couple of the issues tended to in WLAN investigating. Most system examination merchants, for example, Network Instruments, Network General, and Fluke, offer WLAN investigating apparatuses or functionalities as a major aspect of their product offering.

## II. SECURITY GOALS FOR WIRELESS NETWORK

### *Accessibility*

Guarantees survivability notwithstanding Denial of Service (DOS) assaults. On physical and media access control layer assailant can utilize sticking procedures to meddle with correspondence on physical channel. On system layer the assailant can disturb the steering convention. On higher layers, the aggressor could cut down abnormal state administrations e.g.: key administration.

### *Secrecy*

Guarantees certain data is never revealed to unapproved elements.

### *Reliability*

Message being transmitted is never tainted.

### *Substantiation*

Empowers a hub to guarantee the character of the associate hub it is corresponding with. Without which an assailant would mimic a hub, in this way increasing unapproved access to asset and delicate data and meddling with operation of different hubs.

### *Non-Repudiation*

Ensures that the origin of a message cannot deny having sent the message.

***Non-Impersonation***

No one else can pretend to be another authorized member to learn any useful information.

***Attacks using Fabrication***

Generation of false routing messages is termed as fabrication messages. Such attacks are difficult to detect.Now I am giving a brief summary on various wireless networks. These are as:

***Wi- Max***

Overall Interoperability for Microwave Access (WiMAX) is a developing settled broadband remote innovation that will convey last mile broadband network in a bigger geographic zone than Wi-Fi. It is relied upon to give scope anywhere in the range of one to six miles wide. Such WiMax scope reach is required to give altered and migrant remote broadband network without essentially having a line-of-site (LOS) with a base station. WiMAX will likewise empower more prominent portability, higher velocity information applications, reach and throughput than its partner, Wi-Fi. Wi-MAX (Worldwide Interoperability for Microwave Access) give a Point-to-Multipoint-Wire Wireless Network innovation, while loaded with the comforts and favourable circumstances depicted above has its offer of destructions. For a given systems administration circumstance, remote Systems may not be alluring for various reasons. The majority of these need to do with the natural confinements of the innovation. The burdens of utilizing a remote system are: Security, Range, Reliability, and Speed. Remote Networks exhibit a large group of issues for system chiefs. Unapproved access focuses, telecasted SSIDs, obscure stations, and ridiculed MAC locations are only a couple of the issues tended to in WLAN investigating. Most system examination sellers, for example, System Instruments, Network General, and Fluke, offer WLAN investigating devices or

Functionalities as a major aspect of their item line.ess system network which works inside of a scope of 2 to 66 GHz. Security is actualized in the alleged Privacy Sub layer of the Reference Model. In the accompanying, some vital components of the IEEE 802.16 Security Architecture will be displayed. Wi-MAX is the rising broadband remote advancements taking into account IEEE 802.16 models. The security sub layer of the IEEE 802.16d [8] standard characterizes the security components for altered and IEEE 802.16e [9] standard characterizes the security instruments for portable system. The security sub layer backings the three things which are-

(i) validate the client when the client enters in a system,

(ii) (ii) approve the client, if the client is provisioned by the system administration supplier, and afterward

(iii) (iii) it additionally give the important encryption backing to the key exchange and information activity. As WiMAX backings Line of Sight (LOS) and Point to Multi Point (PMP) higher recurrence (10-66 GHz) to lower frequencies (2-11 GHz) and NLOS portable frameworks the security issues expanded immensely, furthermore, WiMAX utilizes radio channels which are open channels and thus represent an intense security issue for movement classification and honesty.

***Wimax Security Features***

***1) Protection Association***

A security affiliation (SA) is an arrangement of security data parameters that a BS and one or a greater amount of its customer SSs offer. Every SA has its own identifier SAID) furthermore contains a cryptographic suite identifier for chose calculations), movement encryption keys (TEKs) and instatement vectors.

***2) Public Key Transportation***

WiMAX

Uses the Privacy and Key Management Protocol (PKM) for secure key management, transfer and exchange between mobile stations. This protocol also authenticates an SS to a BS. The PKM protocol uses X.509 digital certificates, RSA (Rivest -Shamir-Adleman) public-key algorithm and a strong encryption algorithm (Advanced Encryption Standard - AES). The initial draft version of WiMAX uses PKMv1 which is a one-way authentication method and has a risk for Man-in-the middle (MITM) attack. To deal with this issue, in the later version (802.16e), the PKMv2 was used to provide two-way authentication mechanism.

***3) Authorization***

The validation procedure is the approval process in which SS asks for an AK and a SAID from BS by sending an Authorization Request message. This message contains SS X.509 declaration, encryption calculations and cryptographic ID. The BS then interfaces with an AAA (Authentication, Authorization and Accounting) server to accept the solicitation from the SS, and sends back an Authorization Reply which incorporates the AK encoded with the SS's open key, a lifetime key and a SAIS. WiMAX embraces the AES calculation for encryption. ‖The AES figure is determined as various redundancies of change adjusts that change over the data plain-message into the last yield of figure content. Each round comprises of a few handling steps, including one that relies on upon the encryption key. An arrangements of opposite rounds are connected to change ciphertext once again into the first plain-message utilizing the same encryption key‖. Since DES is not any more sufficiently secure, AES is suggested in WiMAX with numerous upheld modes: CCM-Mode and ECB-Mode (in IEEE 802.16-2004), CBC-Mode, CTR Mode, AES-Key-Wrap. WiMAX has been outlined precisely with security concerns however it is still powerless against different assaults.

***Wi-Fi***

Another remote system standard, known as WiFi, is IEEE 802.11 [13]. Because of the utilization of un-authorized recurrence groups (2.4 GHz with 14 unmistakable channels) in IEEE 802.11b/g, giving up to 11/54 Mbps information rate, WiFi systems have increased much consideration. The underlying IEEE 802.11 PHY layer incorporates:

(i) Frequency Hopping Spread Spectrum (FHSS),

(ii) (ii) Direct Sequence Spread Spectrum (DSSS), and

(iii) (iii) Infrared (IR). IEEE 802.11b uses High-Rate DSSS (HR-DSSS), while IEEE 802.11g conveys OFDM. The IEEE 802.11 MAC layer conveys the Distributed Coordination Function (DCF) as a default access method. In this dispute based plan, WiFi STAs connected with the Access Point (AP) utilize their air interfaces for detecting channel accessibility. In the event that the channel is unmoving, the source STA sends its information to the destination STA through the related AP. On the off chance that more than one STA attempt to get to the channel at the same time a crash happens. The standard uses the Carrier Sense Multiple Access/Collision Avoidance (CSMA/CA) component to maintain a strategic distance from impacts [14]. Point Coordination Function (PCF) is another strategy that might be utilized as a part of the MAC layer. In PCF, the information transmission is mediated in two modes: (i) concentrated mode, where the AP surveys each STA in a round-robin style, and (ii) dispute based mode, which works comparatively to DCF. What's more, the Request to Send (RTS)/Clear to Send (CTS) component are connected to take care of the concealed hub issue.

### *MANETs*

To start with, Department of Defense (DOD) did the majority of the examination on Ad Hoc systems for their utilization in military applications in combat zone territories. DARPA subsidized a Packet Radio Network Program, which utilized show radios for transferring information over multi bounce portable systems. Its motivation was to accommodate sharing data transfer capacity and for operation under element conditions. Around then the radios were substantial and power hungry. The Survivable Radio Network (SURAN) undertaking was supported by DARPA in 1980s to build up an arrangement of versatile impromptu system (MANET) radio-switches, to conquer the impediments of Packet Radio Networks. The primary objectives were to build up a little, minimal effort, low-control radio that would bolster more refined parcel radio conventions than the DARPA Packet Radio venture, create and exhibit calculations that could scale to a huge number of hubs and create and show methods for powerful and survivable bundle organizing in advanced electronic assaults. MANET is a self-sufficient arrangement of portable hubs associated by remote connections, where interchanges are regularly accomplished by multi-bounce joins. In a MANET, it is accepted that the hubs are allowed to move haphazardly while having the capacity to speak with each other without the assistance of existing system foundation; a MANET is appropriate for some circumstances where it is not achievable to construct a framework for conveying a system. A few illustrations are combat zone interchanges, portable conferencing, individual region systems, crisis administrations, and sensor systems. The vast majority of work on MANET has been on steering convention. For the correlation of directing conventions, numerous portability models for MANET have been produced. Nonetheless, the accessibility of a wide range of portability models without bound together quantitative measure of the versatility have made it extremely hard to think about the after effects of two free execution investigations of steering conventions.

### *Security Features of MANETs*

#### *1) Availability*

The term Availability means that a node should maintain its ability to provide all the designed services regardless of the security state of it. This security criterion is challenged mainly during the denial-of-service attacks, in which all the nodes in the network can be the attack target and thus some selfish nodes make some of the network services unavailable, such as the routing protocol or the key management service

#### *2) Integrity*

Integrity guarantees the identity of the messages when they are transmitted. Integrity can be compromised mainly in two ways [18]

- **Wicked altering**
- **Unplanned altering**

A message can be removed, replayed or revised by an adversary with malicious goal, which is regarded as malicious altering; on the contrary, if the message is lost or its content is changed due to some benign failures, which may be transmission errors in communication or hardware errors such as hard disk failure, then it is categorized as accidental altering.

#### *3) Confidentiality*

Confidentiality means that certain information is only accessible to those who have been authorized to access it. In other words, in order to maintain the confidentiality of some confidential information, we need to keep them secret from all entities that do not have the privilege to access them.

#### *4) Dependability*

Genuineness is basically affirmation that members in correspondence are real and not impersonators [19]. It is vital for the correspondence members to demonstrate their ways of life as what they have guaranteed utilizing a few strategies in order to guarantee the genuineness. In the event that there is not such a validation system, the foe could mimic a generous hub and in this manner access secret assets, or even proliferate some fake messages to irritate the ordinary system operations.

### *Wireless Sensor Network*

A remote sensor system (WSN) comprises of spatially appropriated independent sensors to screen physical or ecological conditions, for example, temperature, sound, vibration, weight, mugginess, movement or poisons and to agreeably go their information through the system to a fundamental area. The more advanced systems are bi-directional, additionally empowering control of sensor action. The advancement of remote sensor systems was persuaded by military applications, for example, front line reconnaissance; today such systems are utilized as a part of numerous modern and customer applications, for example, mechanical procedure checking and control, machine wellbeing observing, thus on.

***Security in WSN***

***1) Data Confidentiality***

- Information privacy is the most vital issue in system security. Each system with any security canter will commonly address this issue first. In sensor organizes, the secrecy identifies with the accompanying: A sensor system ought not spill sensor readings to its neighbours. Particularly in a military application, the information put away in the sensor hub might be profoundly touchy.
- In many applications nodes communicate highly sensitive data, e.g., key distribution; therefore it is extremely important to build a secure channel in a wireless sensor network.
- Public sensor information, such as sensor identities and public keys, should also be encrypted to some extent to protect against traffic analysis attacks.

***2) Data Integrity***

With the usage of secrecy, a foe might be notable take data. In any case, this doesn't mean the information is sheltered. The enemy can change the information, in order to send the sensor system into chaos. For instance, a malignant hub might include a few pieces or control the information inside of a parcel. This new bundle can then be sent to the first recipient. Information misfortune or harm can even happen without the vicinity of a vindictive hub because of the cruel correspondence environment. Consequently, information uprightness guarantees that any got information has not been modified in travel.

***3) Data Freshness***

Even if confidentiality and data integrity are assured, we also need to ensure the freshness of each message. Informally, data freshness suggests that the data is recent, and it ensures that no old messages have been replayed. This requirement is especially important when there are shared-key strategies employed in the design. Typically shared keys need to be changed over time. However, it takes time for new shared keys to be propagated to the entire network. In this case, it is easy for the adversary to use a replay attack. Also, it is easy to disrupt the normal work of the sensor, if the sensor is unaware of the new key change time. To solve this problem a nonce, or another time-related counter, can be added into the packet to ensure data freshness.

## III. SECURITY MECHANISM

The security components are really used to recognize, keep and recoup from the security assaults. A wide assortment of security plans can be imagined to counter noxious assaults and these can be sorted as high level and low-level. Figure 3 demonstrates the request of security components.

### *A. Low-Level Mechanism*

Low-level security primitives for securing sensor systems incorporates,

1. Key foundation and trust setup
2. Mystery and validation
3. Security
4. Vigour to correspondence foreswearing of administration
5. Secure steering
6. Versatility to hub catch

***1) Key establishment and trust setup***

The essential necessity of setting up the sensor system is the foundation of cryptographic keys. For the most part the sensor gadgets have restricted computational force and people in general key cryptographic primitives are excessively costly, making it impossible to take after. Key-foundation methods need to scale to connect with hundreds or a huge number of hubs. Furthermore, the correspondence examples of sensor systems contrast from conventional systems; sensor hubs might need to set up keys with their neighbours and with information conglomeration hubs. The disservice of this methodology is that aggressors who traded off adequately and numerous hubs could likewise remake the complete key pool and break the plan.

***2) Secrecy and authentication***.

The vast majority of the sensor system applications require assurance against listening stealthily, infusion, and alteration of parcels. Cryptography is the standard barrier. Surprising framework exchange offs emerge while fusing Cryptography into sensor systems. For point-to-point correspondence, end-to-end cryptography accomplishes a abnormal state of security however requires that keys be set up among all end focuses and be contradictory with uninvolved interest and nearby show. Join layer cryptography with a system wide shared key rearranges key setup and backings aloof cooperation and nearby show, however middle of the road hubs may listen stealthily or adjust messages. The soonest sensor systems are prone to utilize join layer cryptography, since this methodology gives the best simplicity of organization among at present accessible system cryptographic approaches.

***3) Privacy***

Like other customary systems, the sensor systems have additionally constrain protection concerns. At first the sensor systems are sent for authentic reason may thusly be utilized as a part of unexpected ways. Giving attention to the vicinity of sensor hubs and information procurement is especially critical.

***4) Robustness to communication denial of service***

An enemy endeavors to upset the system's operation by TV a high-vitality signal. On the off chance that the transmission is sufficiently effective, the whole framework's correspondence could be stuck. More advanced assaults are additionally conceivable; the foe may repress correspondence by disregarding the 802.11 medium access control (MAC) convention by, say, transmitting while a neighbor is likewise transmitting or by consistently asking for channel access with a solicitation to send signal.

***5) Secure routing***

Directing and information sending is a critical administration for empowering correspondence in sensor systems. Sadly, current steering conventions experience the ill effects of numerous security vulnerabilities. For instance, an assailant may dispatch dissent of-administration assaults on the steering convention, anticipating correspondence. The most straightforward assaults include infusing malevolent directing data into the system, bringing about steering irregularities. Basic verification may watch

### *B. High-Level Mechanism*

High-level security mechanisms for securing sensor networks, includes secure group management, intrusion detection, and secure data aggregation.

***1) Secure group management***

Every single hub in a remote sensor system is constrained in its processing and correspondence capabilities. However, intriguing in-system information accumulation and examination can be performed by gatherings of hubs. For instance, a gathering of hubs may be in charge of together following a vehicle through the system. The real hubs involving the gathering might change constantly and rapidly. Numerous other key administrations in remote sensor systems are additionally performed by gatherings. Thus, secure conventions for gathering administration are required; safely conceding new gathering individuals and supporting secure gathering correspondence. The result of the gathering key calculation is ordinarily transmitted to a base station. The yield must be verified to guarantee it originates from a legitimate gathering.

***2) Intrusion detection***

Remote sensor systems are helpless to numerous types of interruption. Remote sensor systems require an answer that is completely appropriated and reasonable as far as correspondence, vitality, and memory prerequisites. The utilization of secure gatherings might be a promising methodology for decentralized interruption detection.

***3) Secure data aggregation***

One advantage of a wireless sensor network is the fine grain sensing that large and dense sets of nodes can provide. The sensed values must be aggregated to avoid overwhelming amounts of traffic back to the base station. For example, the system may average the temperature of a geographic region, combine sensor values to compute the location and velocity of a moving object, or aggregate data to avoid false alarms in real-world event detection. Depending on the architecture of the wireless sensor network, aggregation may take place in many places in the network. All aggregation locations must be secured.

## IV. CHALLENGES OF SENSOR NETWORKS

The way of substantial, specially appointed, remote sensor systems presents critical difficulties in outlining security plans. A remote sensor system is an exceptional system which has numerous imperative contrasted with a customary PC system.

### *A. Wireless Medium*

The remote medium is naturally less secure on the grounds that its show nature makes listening in basic. Any transmission can without much of a stretch be captured, adjusted, or replayed by a foe. The remote medium permits an aggressor to effortlessly block substantial parcels and effectively infuse vindictive ones. Despite the fact that this issue is not one of a kind to sensor systems, conventional arrangements must be adjusted to productively execute on sensor systems.

### *B. Ad-Hoc Deployment*

The impromptu way of sensor systems implies no structure can be statically characterized. The system topology is constantly subject to changes because of hub disappointment, expansion, or portability. Hubs might be conveyed via airdrop, so nothing is known of the topology before arrangement. Since hubs might fall flat or be supplanted the system must bolster self-arrangement. Security plans must have the capacity to work inside of this dynamic environment.

### *C. Hostile Environment*

The following testing variable is the antagonistic environment in which sensor hubs capacity. Bits confront the likelihood of pulverization or catch by aggressors. Since hubs might be in an unfriendly domain, assailants can without much of a stretch addition physical access to the gadgets. Assailants might catch a hub, physically dismantle it, and concentrate from it profitable data (e.g. cryptographic keys). The exceptionally threatening environment speaks to a genuine test for security specialists.

### *D. Resource Scarcity*

The compelling asset impediments of sensor gadgets posture impressive difficulties to asset hungry security instruments. The equipment requirements require to a great degree effective security calculations as far as transfer speed, computational many-sided quality, and memory. This is no insignificant errand. Vitality is the most valuable asset for sensor systems. Correspondence is particularly costly as far as force. Unmistakably, security components must give unique push to be correspondence effective keeping in mind the end goal to be vitality proficient.

### *E. Immense Scale*

The proposed size of sensor systems represents a huge test for security instruments simply networking tens to a huge number of hubs has turned out to be a considerable undertaking. Giving security over such a system is similarly testing. Security instruments must be versatile to extensive systems while keeping up high calculation and correspondence productivity.

### *Unreliable Communication*

Positively, inconsistent correspondence is another risk to sensor security. The security of the system depends intensely on a characterized convention, which thus relies on upon communication.

- ***Unreliable Transfer****:* Normally the packet-based routing of the sensor network is connectionless and thus inherently unreliable.
- ***Conflicts****:* Even if the channel is reliable, the communication may still be unreliable. This is due to the broadcast nature of the wireless sensor network.
- ***Latency****:* The multi-hop routing, network congestion and node processing can lead to greater latency in the network, thus making it difficult to achieve synchronization among sensor nodes.

### WORK PLAN

In this research I am working on wireless security trends and how to protect data over wireless network, In this I am discuss in the details about the wireless applications. And the use of different standard and protocols & security parameters mentioned below:

1. Core security tended to the physical security issue and guaranteed ii is accomplished utilizing two fundamental strategies: First accomplishment was clone by rolling out document framework level improvements creating another record framework design with appropriate encryption and access controls, Second accomplishment on this layer was remote access to the framework utilizing secure channel. Open private key pair approach was utilized to permit just a predefined set of machines to have inner access.
2. Security Information System concentrated on log joining utilizing MYSQL database and giving a Command Line Interface manufactured utilizing shell scripts and Graphical User Interface executed utilizing PHP. This layer produced reports and itemized examination of system logs. This layer goes about as the heart of the system by planning the usefulness and giving simple to utilize interfaces to information catch.

## V. CONCLUSIONS

This paper analyzes different wireless network and their security concern. The paper presents different security features of various wireless networks. Due to distinct feature of different network, each network must offer different security issues. But there are some common issues due to common security goals. That‘s why a common algorithm can be developed to secure these different wireless networks.

### REFERENCES

[1] B.Daya, (2013) “Network Security History, Importance, and future” International Journal of Advance Foundation and Research in Science & Engineering, Volume 1, Issue 3,

[2] M. A. Shibli,( January 2009) “Magic NET: Human Immune System & Network Security,” IJCSNS International Journal of Computer Science and Network Security, Vol. 9 No.1,.

[3] R. K. Khalil,( 2010) “A Study of Network Security Systems,” IJCSNS International Journal of Computer Science and Network Security,.

[4] S. Alabady, (2009) “Design and Implementation of a Network Security,” Technology, Vol. 1,p. 11,.

[5] Dr. Gurjeet Singh (April 2012) “Security Issues in Wireless Broadband Networks” Volume 12 Issue 5 Version 1.0, Double Blind Peer Reviewed International Research Journal

[6] Sikkens B. (2008). Security Issues and proposed solutions concerning authentication and authorization for WiMax. 8th twente student Conference on IT.

[7] International Journal of Grid Distribution Computing Vol.7, no.3 (2014), pp.23-28 http://dx.doi.org/10.14257/ijgdc..7.3.03.

[8] Giruka,(2008) V.C., *et al.*,. Security in wireless sensor 9. Kalita, H.K. and A. Kar, 2009. Wireless sensor networks. Wireless communications and mobile network security analysis. International Journal of computing, 8(1): 1-24.

[9] Jain, M.K., 2011. Wireless sensor networks: 10. Ning, P., A. Liu and W. Du, 2008. Mitigating DoS Security issues and challenges. International Journal attacks against broadcast authentication in wireless of Computer and Information Technology, sensor networks. ACM Transactions on Sensor 2(1): 62-67

[10] Lewis, F.L., (2004), “Security Issues and Attacks in Wireless Sensor Network”**,** World Applied Sciences Journal 30 (10): 1224-1227.

[11] Giruka, V.C., *et al.*, 2008.Security in wireless sensor networks. Wireless communications and mobile computing, 8(1): 1-24.

[12] R. L. Rivest, “The RC5 Encryption Algorithm”, in Proc. 1994 Leuven Workshop on Fast Software Encryption,1995, pp. 86.96.

[13] C. Karlof, N. Sastry, and D. Wagner. Tinysec: link layer security architecture for wireless sensor networks. In SenSys 04: Proceedings of the 2nd international conference on Embedded networked sensor systems, pages162.175, New York, NY,USA, 2004. ACM Press.

[14] B. Kadri, A. Mhamed, and M. Feham "Secured Clustering Algorithm For Mobile Ad Hoc Networks", International Journal of Computer Science and Network Security, Vol.7, No.3, pp 27-34.2007.

[15] J. Albath, and S. Madria. "Practical Algorithm for Data Security (PADS) in Wireless Sensor Networks".MobiDE’07, , Beijing, China.2007.

[16] Tai-hoon Kim, International Journal of Multimedia and Ubiquitous Engineering Vol. 3, No. 3, July, 2008 77 Wireless Network Security: Vulnerabilities, Threats and Countermeasures.

[17] Chang-Su Moon,(2014) “ A Study on the Integrated Security System based Real-time Network Packet Deep Inspection” International Journal of Security and Its Applications Vol.8, No.1 (2014), pp.113-122.

[18] Ashwani Kush, Phalguni Gupta, Ram Kumar, “Performance Comparison of Wireless Routing Protocols”, Journal of the CSI, Vol.35 No.2, April-June 2005.

[19] Ashwani Kush “A Survey of Routing Protocols in Mobile Ad Hoc Networks” International Journal of Innovation, Management and Technology, Vol. 1, No. 3, August 2010.

[20] Dr. G. Padmavathi, Mrs. D. Shanmugapriy “A Survey of Attacks, Security Mechanisms and Challenges in Wireless Sensor Networks” (IJCSIS) International Journal of Computer Science and Information Security,Vol. 4, No. 1 & 2, 2009

[22] Atish Mishra, Arun Kumar Jhapate, Prakash Kumar “Designing Rule Base for Genetic Feedback Algorithm Based Network Security Policy Framework using State Machine”, ICCD 2009: 2009 International Conference on Computer Design and Applications, May 2009

[23] Ramy K. Khalil, Fayez W. Zaki, June 2010 “A Study of Network Security Systems” IJCSNS International Journal of Computer Science and Network 204 Security, VOL.10 No.6

[24] Promila, Dr. R. S. Chhillar, Sep.-Oct. 2012 “Review of WI-FI Security techniques**”** International Journal of Modern Engineering Research (IJMER) Vol. 2, Issue. 5,

[25] Rajesh Pant, CN Khairnar (April 2014) “A Cumulative Security Metric for an Information Network” International Journal of Application or Innovation in Engineering & Management (IJAIEM) Volume 3, Issue 4.

[26] Shio Kumar Singh , M P Singh , and D K Singh(May to June Issue 2011)”A Survey on Network Security and Attack Defense Mechanism For Wireless Sensor Networks” International Journal of Computer Trends and Technology.

[27] Swati Sukhija, Shilpi Gupta (January 2012) “wireless network security protocols A comparative study” International Journal of Emerging Technology and Advanced Engineering Volume 2, Issue 1.

[28] A. Antony Vinoth, Kumar, C.Karthikeyan, V.Karthikeyan (December 2012) “An Innovative wireless network security for air force using wireless protocols” International Journal of Scientific and Research Publications, Volume 2, Issue 12,

[29] Wang Yong and Hu Yitao (2014) “Study on prediction of network security situation based on fuzzy neutral network”Journal of Chemical and Pharmaceutical Research.

[30] Huang Zhilong. Research on computer network security analysis model [J]. Research on computer network security analysis model , 2014(05).

[31] Zhang Tao; Hu Mingzeng; Yun Xiaochun, Zhang Yongzheng. Research on computer network security analysis model [J]. *Journal of communications*, **2005**.