International Journal on Recent and Innovation Trends in Computing and Communication
Volume: 5 Issue: 6

ISSN: 2321-8169
689 – 692

A Pragmatic Review on Security and Integrity in Wireless Networks

Shina Arora
Education Consultant
Hoshiarpur, Punjab, India
shinacgc@rediffmail.com

Abstract— Wireless transmission is one of the prominent and widely used aspects for remote and trust based networks. A wireless network encompass of a set of arbitrary as well virtually connected devices using wireless transmission media. It includes assorted but compatible set of protocols so that the communication can be done with security, integrity and higher accuracy. In wireless networks, there are two key segments as "Mobile ad hoc networks (MANET) and Wireless Sensor Networks (WSN)" using which the data transmission can be established between numbers of mobile nodes called as motes. In wireless networking, there are number of dimensions in which efficiency and quality of service is a key issue. Such aspects are energy optimization, security, cryptography, routing, scheduling, cost factor and many others. Security is one of the key domains that is considered as sensitive and most addressed domains because of many applications of wireless networks in defense, corporate sector and related sensitive domains. Till now, there are number of protocols and an algorithm using encryption and hash keys but still this area is under research. In this research manuscript, an empirical review on assorted security protocols and algorithms is presented and it is extracted that a novel multilayered algorithm can be devised, developed and proposed having the concept of dynamic hash key based generation of cryptography. Using this unique and effective approach, the overall security, integrity and performance of the wireless scenario can be improved as compared to the classical approach.

Keywords- *Vulnerability, Security, Wireless Sensor Networks, Cryptography, Encryption*

*****

I. INTRODUCTION

In wireless networks, there are mobile nodes which are connected to each other using radio or related transmission line without any physical infrastructure. Wireless Network refers to a specific scenario having mobile nodes connected via mobile routers, base stations or satellites using which the overall network can be controlled and monitored. There are number of applications in which wireless sensor networks are integrated. In classical way, the wireless networks are implemented for the ease of mobility, remote accessibility and cross region connectivity. One of the traditional real life implementation is vehicular ad hoc networks (VANET) in which the vehicles are equipped with wireless devices. In this scenario, the minimum distance of vehicles on road can be measured at run time which reduces the scope of any catastrophe on road.

In WiMax (Worldwide Interoperability for Microwave Access), that is one of the high speed communication of around 40 Mbps is widely used for remote access. It provides high speed integrity based delivery of broadband access to the multiple and remote locations.

The key attribute of a Wireless Network comprises

Source	–	Source Node (Mote)
CH	–	Cluster Head (Aggregator)
BS	–	Base Station (Tower)

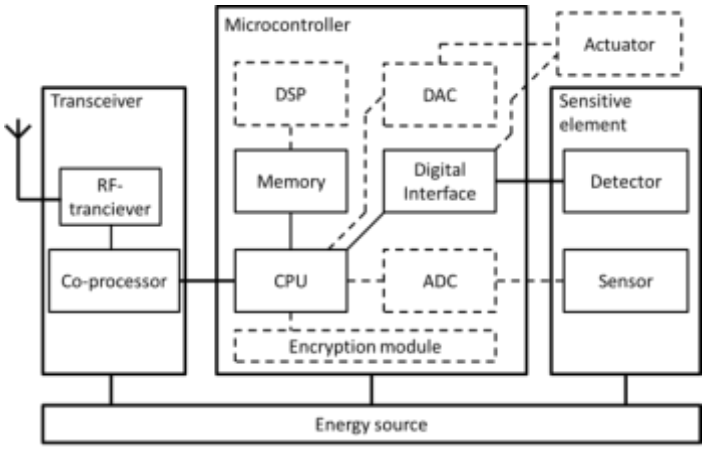

Figure 1 – Components of a typical Wireless Sensor Node

Each device or mobile node in a wireless scenario is having mobility and moves arbitrarily for data transmission with higher efficiency and integrity.

Table 1 – Comparison between WSN and Mobile Ad Hoc Networks

WIRELESS SENSOR NETWORKS	MOBILE AD HOC NETWORKS
Energy Consumption more and generally non rechargeable due to remote and sensitive locations	Energy is not the issue because of recharging
Very far and not accessible physically in general	More close of Human Experts / Users
Data Aggregation / Grouping	No need of aggregation
Clustering	Each mobile node act as router itself
Security and Integrity are the key issues	Security is not an issue as it is always very close to human user

Taxonomy of Wireless Technology Networks

- Wireless LAN
- Wireless WAN
- Wireless Mesh Network
- Wireless PAN
- Wireless MAN
- Cellular Network
- Global Area Network
- Space Network

Features of Wireless Networks

- Autonomous
- Dynamic and Effective Load Balancing
- Scalability
- Network Access Control
- Distributed, Arbitrary and Connected Operations
- Multihop based Routing
- Network Topology in Dynamic
- Network Scalability
- Light Weight Terminals
- Ease and Speed of deployment
- Decreasing dependency on infrastructure
- Mobility and Quality of Service
- Portability and Transportation

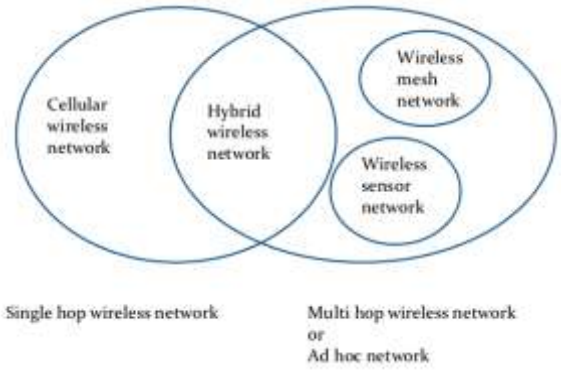

Figure 2 - Taxonomy of Wireless Networks

VULNERABILITIES AND SECURITY LOOPHOLE IN WIRELESS NETWORKS

- **Eavesdropping** - Interception and accessing the messages or conversations by unauthentic users.
- **Wormhole attack –** It refers to the creation of a new and fake hole or gateway from which the malicious packets can be transmitted
- **Blackhole attack –** In this attack the cracker modifies the data packets and fake channel is used for the delivery of signals
- **Byzantine attack –** Non optimal or simply long path is used by the attacker so that there is more overhead and higher delay in the transmission line
- **Rushing attack -** Two charmed aggressors use the tunnel philosophy to outline a wormhole. If a fast transmission way exists between the two terminations of the wormhole, the tunneled groups can multiply speedier than those through a standard multi-hop route.
- **Jamming** – It is considered as DDoS **(Distributed Denial of Service)** attack that choke the network path or complete channel to push back the genuine traffic

II. LITERATURE SURVEY

For deep and empirical analysis of the security and integrity aspects in wireless networks, a number of research papers are analyzed from various sources. Following are the approaches and conclusions of research papers and manuscripts.

[1] In this paper, a novel and effective approach for the energy encryption is addressed. The approach is associated with WPT (Wireless Power Transfer) for improving the overall performance of the network in terms of security and integrity. The proposed approach is uses dynamic, secured and authorization based energy consumption so that the overall performance of network can be enhanced.

[2] In this research manuscript, an effective and high performance approach for security in clustered wireless

environment is proposed. This approach used is query process based paradigm to implement the security in wireless networks. Using the proposed approach in this paper, the security and integrity is preserved on multiple parameters against various attacks

[3] In this paper, the authors address the use and integration cryptographic hash approaches for implementation of security and authentication in wireless networks. This work underlines and implements MD5 (Message Digest) and SHA (Secured Hash Algorithm) as a hybrid algorithm to ensure and enhance the security in wireless networks

[4] In this work, the lightweight cryptography is implemented for security and privacy issues in the wireless networks. A unique and effective ultra lightweight approach KLEIN to improve the overall efficiency of the network environment is proposed and implemented.

[5] Homomorphic Encryption is the base issue taken in this work. In this paper, the authors implemented symmetric encryption and homomorphic encryption for performance evaluation. Finally, it is found and concluded that the performance cannot be highly improved using homomorphic encryption approaches

[6] In this paper, the authors propose a lightweight hash, Neeva-hash fulfilling the especially critical considered lightweight cryptography. Neeva-hash depends on upon wipe method for cycle with programming liberal change which gives excellent ability and required security in RFID progression. The proposed hash can be utilized for some application based purposes.

[7] The work in this paper addresses the issues of WSN requests and lightweight security. This paper addresses and devises a new approach for security and integrity in the wireless networks.

[8] This work considers two applications: “hop by hop transmission of information from cluster nodes to the base station and direct communication to clustered nodes information by mobile clients by strategy for mobile gadgets. Because of the hardware blocks of WSNs, some irrelevant effort operations, for occurrence, symmetric cryptographic approaches and hash functions points are utilized to finish a dynamic key association. The session key can be redesigned to keep dangers of assault from every correspondence. With these strategies, the information accumulated in wireless sensor networks can be all the more safely gave. Additionally, the proposed plan is dejected down and separated and related game plans”. In addition, a NS2 era is made in which the exploratory results demonstrate that the designed correspondence convention is workable.

[9] In this paper, the issue of key management is addressed for security and integrity in the wireless environment. The key goal of this research manuscript is to evaluate, compare and extract the suitable and high performance protocol for the wireless scenarios.

[10] To address the objectives of security and respectability, this paper proposes a lightweight module considering the robust operations. The proposed cryptographic game plan utilizes elliptic turn focuses to attest the going on focus focuses and as one of the puzzled helper parameters to make the pseudorandom bit movement. This social occasion is utilized as a bit of XOR, change and creamer operations with a specific completed target to encode the information pieces. The trial results in light of Mica2 sensor bit display that the proposed encryption game plan is nine times complex than the LED custom and two times speedier than the TWINE convention. The authors have also performed distinctive certain tests and cryptanalytic assaults to study the security way of the calculation and found the figure provably secure.

III. CRYPTOGRAPHY AND SECURITY ASPECTS

Cryptography is one of oldest and widely used approach for encryption of data and signals. Using this approach, any data signal or group of packets can be encrypted so that they can be transmitted in secured way. A number of algorithms devised by number of researchers, still this domain is under research.

Key Advantages of using Cryptography includes

- Integrity based transmission
- Push back capability of the crackers
- Secured authentication
- Trust Based Communication

DES (Data Encryption Standard) – This is superior encryption or security based standard to be endorsed by NIST. It relies on upon the IBM proposed number called as Lucifer. This changed into the standard of year 1977. By that instance, distinctive strikes as well as strategies recorded endeavor of deficiencies in DES that made a questionable square figure. It is far better than XOR based simple encryption. This is not covered under group based ciphers.

3DES: As an improved and enhanced version of DES, the Triple DES encryption standard got integrated and proposed. The approach was 3 times better and effective than the previous work. In any case, triple DES is not effective and very slow as compared to other approaches.

AES or simply Advanced Encryption Standard refers to a novel standard for encryption upheld by the NIST for supplant

DES. The algorithm devised in year 1997 after constraint for selection of the effective encryption method.

Blowfish: It is one of the effective approached in the most overall saw open space encryption approaches. Blowfish algorithm first integrated in year 1993 rejecting the way that it encounters delicate keys issue, no strike is known not gainful against.

Algorithm	MB/Second
Blowfish	63.386
Rijndael on 128 b key	60.010
Rijndael on 192 b key	52.145
Rijndael on 256 b key	47.229
Rijndael on 128 for CTR	56.710
Rijndael on 128 for OFB	51.925
Rijndael on 128 for CFB	46.601
Rijndael on 128 for CBC	54.447
DES	20.340
(3DES)DES-XEX3	19.783
(3DES)DES-EDE3	9.748

CONCLUSION AND SCOPE OF FUTURE WORK

There are number of algorithms and approaches for encryption and dynamic cryptography. Still, there is need to propose, devise and implement the salt based hybrid and dynamic cryptography so that the higher level of security and integrity can be proposed. The networks should be secured with the design of a new algorithm using hybrid cryptography approach for security in the wireless base control station. The current cryptography approaches can be made hybrid and high performance using metaheuristic approaches including Ant Colony Optimization, Honeybee Algorithm, Firefly Algorithm, River Formation Dynamics and many others.

REFERENCES

[1] Zhang, Z., Chau, K.T., Qiu, C. and Liu, C., 2015. Energy encryption for wireless power transfer. *Power Electronics, IEEE Transactions on*, *30*(9), pp.5237-5246.

[2] Ghosal, A. and DasBit, S., 2015. A lightweight security scheme for query processing in clustered wireless sensor networks. *Computers & Electrical Engineering*, *41*, pp.240-255.

[3] Kumar, M., A Light Weight Cryptographic Hash Algorithm for Wireless Sensor Network.

[4] Li, W., 2015. An Ultra-Lightweight Side-Channel Resistant Crypto for Pervasive Devices.

[5] Ramotsoela, T.D. and Hancke, G.P., 2015, August. Data aggregation using homomorphic encryption in wireless sensor networks. In *Information Security for South Africa (ISSA), 2015* (pp. 1-8). IEEE.

[6] Bussi, K., Dey, D., Kumar, M. and Dass, B.K., 2016. Neeva: A Lightweight Hash Function.

[7] Kiruthika, B., Ezhilarasie, R. and Umamakeswari, A., 2015. Implementation of the Modified RC4 Algorithm for Wireless Networks. *Indian Journal of Science and Technology*, *8*(S9), pp.198-206.

[8] Chen, C.L., Chen, C.C. and Li, D.K., 2015. Mobile Device Based Dynamic Key Management Protocols for Wireless Sensor Networks. *Journal of Sensors*, *2015*.

[9] Rajeswari, S.R. and Seenivasagam, V., 2016. Comparative Study on Various Authentication Protocols in Wireless Sensor Networks. *The Scientific World Journal*, *2016*.

[10] Biswas, K., Muthukkumarasamy, V. and Singh, K., 2015. An Encryption Scheme Using Chaotic Map and Genetic Operations for Wireless Sensor Networks. *Sensors Journal, IEEE*, *15*(5), pp.2801-2809.