International Journal of Computing and Corporate Research
ISSN (Online) : 2249-054X
Volume 4 Issue 5 September 2014
International Manuscript ID : 2249054XV4I5092014-7

A PRAGMATIC REVIEW ON THE SECURITY AND INTEGRITY ASPECTS AND RELATED PERFORMANCE ENHANCEMENT IN WI-MAX ENVIRONMENT

Amit Sharma,
Asst. Professor,
School of Information Technology,
Apeejay Institute of Management Technical Campus,
Jalandhar, Punjab, India

ABSTRACT

WiMAX is one of the high speed, trust and integrity based technology with the base technology and protocols of IEEE 802.16. A number of algorithms and secured architectures are developed so far still the domain is under research. The dynamic cryptography and secured handoff is the key aspect in this work. In this paper, a unique homomorphic based security algorithm is proposed to the developed and implemented for higher integrity and less cost factor in WiMax Environment. Using the effective algorithm during region transformation as well as shift, there is need to develop a secured algorithmic approach which can make the handoff more secured and other channel will not be able to access the transmission line.

Keywords - WiMax, Security and Integrity, Dynamic Security Algorithm

FOREWORD

Security and Integrity is one of the key aspects in the wireless system. There is number of approaches, protocols and algorithms to enforce and implement the security in wireless scenarios, still this area is under research. In this work, the pragmatic review on the wimax security and related dimensions are evaluated with the suggestive points.

1. INTRODUCTION

1.1 Wi-Max

As with any other system related to network, security is the key issue and element in the overall WiMAX system. The security in WiMAX is required to be integrated so that it can provide the

International Journal of Computing and Corporate Research
ISSN (Online) : 2249-054X
Volume 4 Issue 5 September 2014
International Manuscript ID : 2249054XV4I5092014-7

sufficient and effective protection repelling against the intrusion and other related types of unauthorised access without any type of hindrance in the overall operation.

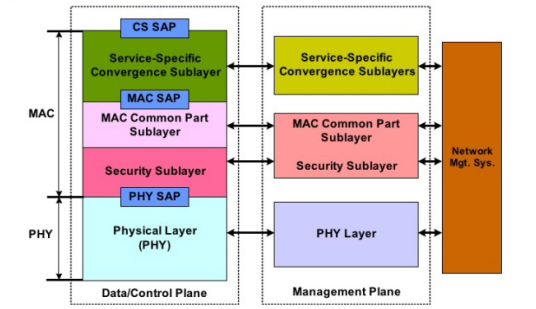

Fig. 1 - 802.16 Protocol and Standard

Difference between assorted wireless technologies are -

Table 1 - Features and Related Dimensions of WiMax and WiFi Technologies

Key Feature and Aspect	WiMax Technology 802.16a	Wi-Fi Technology 802.11b	Wi-Fi Technology 802.11a/g
Primary and Key Application	Wireless Broadband Access	WLAN	WLAN
Frequency Band	2-11 GHz	2.4 G Hz ISM	2.4 GHz ISM (g) 5 GHz U-NII (a)
Bandwidth of Channel	Adjustable / Customizable 1.25 - 20 MHz	25 MHz	20 MHz
Duplex Status	Full Duplex	Half Duplex	Half Duplex
Radio Technology	OFDM (256-channels)	Direct Sequence Spread Spectrum	OFDM (64-channels)
Bandwidth Efficiency	Less than Equal to 5 bps/Hz	Less than Equal to 0.44 bps/Hz	Less than Equal to 2.7 bps/Hz
Modulation	BPSK, QPSK, 16-, 64-, 256-QAM	QPSK	BPSK, QPSK, 16-, 64-QAM
FEC	Convolution Code Reed-Solomon	No	Convolution Code
Encryption	3DES AES	RC4	RC4
Mobility	Mobile WiMax	Under development	Under development
Mesh Support	Present	Proprietary	Proprietary
Access Protocol	Request and Grant	CSMA/CA	CSMA/CA

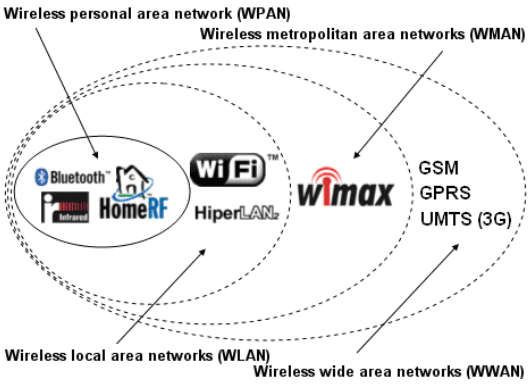

Fig. 2 – Taxonomy of Wireless Technologies

International Journal of Computing and Corporate Research
ISSN (Online) : 2249-054X
Volume 4 Issue 5 September 2014
International Manuscript ID : 2249054XV4I5092014-7

Table 2 – Comparative Pragmatic Analysis of Wireless based Standards

	Bluetooth	Wi-Fi (a)	Wi-Fi (b)	Wi-Fi (g)	Wi-MAX
International Standard	802.15	802.11 a	802.11 b	802.11 g	802.16
Frequency (GigaHz)	2.5	5	More than 2	2.4	2 - 66
Speed (Mbps)	Around 1	54	11	More than 50	Around 100
Range Parameter (mt)	10	More than 50	More than 80	More than 100	More than 50
Advantages	Low Cost	Speed	Less Cost	Speed	Range
Limitations	Range Issues	Cost Factor	Speed	Cost and Range both	Cost

1.2 WIMAX SECURITY

WiMAX makes utilization of Internet Protocol (IP) as the key transport system. Because of this, WiMAX security measures need to consolidate not just the traditional security prerequisites for the wireless information transfers system, furthermore those related to the usage of IP systems.

In the light and perspective of requirement for high and compelling level of WiMAX security, IEEE 802.16 working gatherings shaped and joined the security measures in the norms at the time the idea stages to impart and implement the WiMAX security and helplessness dangers. WiMAX security was been inserted into the standard from starting instead of including as additional at a later stage. With the appropriation of this methodology, WiMAX security is executed more compelling while being less meddling to the client.

WiMAX security components are incorporated into the standard and fall under four fundamental headings:

- Authentication of the client gadget
- Higher level client verification
- Advanced over-the-air encryption
- Methods for securing the control and motioning inside an IP situation

1.3 WIMAX SECURITY THREATS

During the development of any system, the security and integrity is very important. It becomes mandatory to understand and evaluate the issues and factors which can affect the security directly or indirectly.

The key threats to WiMAX security are hereby summarized

- **Interception or Eavesdropping** – Unauthentic access of the messages
- **Wormhole or False Gateway Attack –** Creating new or fake gateway for transmission of packets in non legitimate aspects
- **Modification or Blackhole attack –** The intruder creates the cracking attempt for transmission of packets on fake or false channel

- **Non Optimal Path or Byzantine Allocation Attack** – Assignment of longest path rather than shortest to delay the network transmission.
- **Rushing Malware Attack** – Creation of fake or false tunnel to overload the traffic from assorted dimensions.
- **Jamming** – Another type of Distributed Denial of Service attack in which the intruder distributes or access the network resources to non genuine dimension

2. LITERATURE REVIEW

2.1 Literature Survey and Excerpts

[1] Homomorphic based encryption is the classical and key issue addressed and avoided in this work. In this work, the authors performed the implementation using symmetric key encryption as well as homomorphic deployment to improve the overall performance of the system.

[2] This paper is focusing on preserving the basic security features including trust, confidentiality as well as integrity with the protection from assorted attacks including replay and related security issues. In this work, the dimensions and vulnerability levels of the attacks and their impact is investigated and proposed the need of an effective mechanism.

[3] In this paper, an effective one-way, lightweight, cryptography based hash algorithm is suggested with a target to produce a hash-digest with fixed and relatively small length for such an energy-starved wireless network. The primary focus is making the algorithm light-weight so that upon using it in application of network like WSN, the nodes can successfully run the algorithm with low energy. It is suggested that such algorithm must fulfill all the basic properties such as collision resistance in a one-dimensional and uni-way hash algorithmic approach. The proposed algorithm is developed using NS2 simulation tool and results were compared with MD5 and SHA1.

[4] In this research paper, the key effect of the increased packet size is investigated for the Domingo-Ferrer encryption scheme and compared to a symmetric encryption scheme. It was found that the symmetric encryption scheme outperforms the homomorphic encryption scheme for smaller networks, but as the network size grows, homomorphic encryption starts outperforming symmetric encryption. It was also found that the homomorphic encryption scheme does not significantly reduce the performance of plaintext aggregation.

[5] In this research work, the authors presented and depicted the use of lightweight hash, Neeva Hash (NH) satisfying the very basic idea of lightweight cryptography. Neeva-hash is based on sponge mode of iteration with software friendly permutation which provides great efficiency and implemented the security using RFID. The proposed work by the authors is effective for assorted wireless network scenarios.

[6] In this work, various authentication protocols such as key management protocols, lightweight authentication protocols, and broadcast

authentication protocols are compared and analyzed for all secure transmission applications. The major goal of this survey is to compare and find out the appropriate protocol for further research. Moreover, the comparisons between various authentication techniques are also illustrated.

[7] The ultimate aim of this paper is to provide the high level of security without degraded quality of service that is Security Management in Mobile node Wimax. This work distinguish three main groups of applications: 1) safety applications, 2) traffic efficiency applications and 3) infotainment services (non-safety). In this paper, the authors proposed security management in mobile WiMAX without degrading the quality of service in 4G multihop wireless network using the elliptic curve Diffie-Hellman (ECDH) protocol. Finally, the work performs the comparison between the existing trend and the proposed system from the simulation and with the help of graphs.

[8] This work is based on the implementation of a lightweight hash approach Neeva hash that implements the effective cryptography. This approach is solely dependent on the higher security and integrity in the wireless networks.

[9] The authors in this work presented that WSN should be integrated with the lightweight security protocols and there must be dynamic security to remove or avoid the crackers.

[10] In this research work, there are multiple implementations including hop to hop packet transmission with the association of cluster nodes to enforce higher security and integrity during handoff and network updations mode. The work in this paper is making use of network simulator ns2 for assorted topologies to defend the proposed work.

Research Gaps and Proposed Dimensions

- To devise, propose and perform the implementation using salt based hybrid as well as dynamic security based on homomorphic cryptography so that quality of service, security as well as network integrity can be enhanced
- To develop, design and implement a novel multilayered approach with the use of hybrid security for implementing the security in the wireless scenarios
- To investigate and conclude the scope of multi layer attacks.
- To analyze the need and advantages of the proposed approach and detailed comparative analysis.

Homomorphic Security

Homomorphic Cryptography refers to a specific form of Cryptography and obviously the secured layer which permits the computations and measurements dynamic in nature and performed on the ciphertext. It generates the encrypted result which at the time of decryption matches and analyze the results of the operations performed on the plaintext.

The proposed work is entirely based on the security of wi-max based systems in which this type of

International Journal of Computing and Corporate Research
ISSN (Online) : 2249-054X
Volume 4 Issue 5 September 2014
International Manuscript ID : 2249054XV4I5092014-7

dynamic homomorphic cryptography shall be implemented

CRYPTOGRAPHY BASED APPROACHES AND RELATED SECURITY DIMENSIONS

Cryptography or simply encryption is not a new term in technology based scenarios. A number of algorithms, protocols and standards are devised so far by number of academicians, researchers and scientists. Still, this domain is in huge interest for corporate world because the cracking attempts and intruding scenarios are increasing very rapidly.

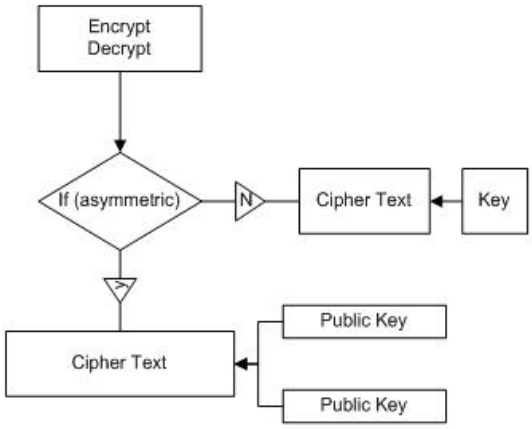

Fig. 3 – Dimensions associated with Cryptography

The advantages and effectiveness of cryptography includes

- Confidentiality
- Integrity
- Authentication
- Validation
- Identification
- Availability
- Dynamic

Following is the diagrammatic view of cryptography in assorted disciplines and domains

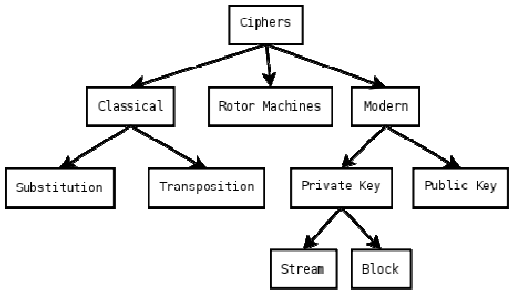

Fig. 4 – Ciphers and related Taxonomy

Following is the list of prominent open source cryptography libraries associated with network technology

- Botan
  - C++
- Bouncy Castle
  - Java
- cryptlib
  - C
- Crypto++
  - C++
- Libgcrypt
  - C
- Libsodium
  - C
- NaCl
  - C, C++
- Nettle

- C
- OpenSSL
  - C
- wolfCrypt
  - C

3.1 Research Methodology for Proposed Outcome

- Generation of the WiMax environment for virtual scenario formation
- Initialize and Activate the parameters and associated aspects in the Wi-Max scenario.
- Initialize the wimax nodes and implementation of handoff
- Activation and Generation of the data packet to be transmitted
- Generation of the security key based on dynamic hash algorithm
- Implementation of existing approach based on the static key
- Implementation of proposed algorithm based on dynamic homomorphic key
- Comparison between classical and proposed approach on multiple parameters
  - Execution Time
  - Cost Factor
  - Efficiency
  - Overall Performance
  - Complexity

CONCLUSION AND SCOPE OF FUTURE WORK

In the classical approach of base paper, there is ECDH algorithm in which the key generation is not dependent on the timestamp and not having dynamic security. In the proposed algorithm, the dynamic key based homomorphic security shall be used with EDCH algorithm.

In the proposed work, the integration of EDCH with homomorphic encryption can enhance the security and overall lifetime of the network. The homomorphic property also implies malleability. This means, if you have some ciphertext, then you can create a different ciphertext with a related plaintext, and this property can be unwanted in this scheme.

REFERENCES

[1] 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.

[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] 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.

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

[6] Rajeswari, S.R. and Seenivasagam, V., 2016. Comparative Study on Various Authentication

Protocols in Wireless Sensor Networks. The Scientific World Journal, 2016.

[7] Security Management in Mobile Node Wimax Without Degrading the Quality of Service (QOS), Arunima kumari, Abhilasha and Mr. N. Prabakaran[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.

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

[9] 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.

[10] 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.