International Journal of Innovative Technology and Exploring Engineering (IJITEE)
ISSN: 2278-3075 (Online), Volume-3 Issue-2, July 2013

An Efficient Secure Communication in WLAN Using DH Method

Islabudeen M, Sathiya M

Abstract— Wireless Local Area Network (WLAN) is one kind of wireless networks and which is a wireless network in limited area where laptop and mobile devices can connect through it freely. WLAN is popular due to its flexibility, mobility and portability and are widely deployed in schools, commercial organizations or in home uses.However, a WLAN suffers from all the constraints of wireless networks including low transmit speed and bandwidth, memory and processing power which limits the implementation of security approaches as can be implemented in wired LANs which includes public-key ciphers. Moreover, due to the feature that signals are transmitted in the air, an adversary can easily monitor and intercept all signals. Thus, robust, efficient and effective security measurements are essential for all WLANs. In this Project, I proposed an efficient encryption technique named Diffie-Hellman Triple key method to guard the management frames that are disseminated from the Access points.It is used to authenticate as well as protect our messages from tampering.

Index Terms—Architecture Model, Key Generation, Key Establishment, Performance.

I. INTRODUCTION

Wireless and mobile networks represent an increasingly important segment of networking investigation as a whole, driven by the hasty growth of transferrable computing, communiqué and implanted devices connected to the Internet. Overall, it is unblemished that mobile, wireless and sensor devices will indeed outnumber wired end-user terminals on the Internet in the adjacent prospect, intensely inspiring deliberation of primarily new network architectures and services to meet changing needs.Over the next 10-15 years[1], it is anticipated that significant qualitative changes to the Internet will be driven by the rapid proliferation of mobile and wireless devices, which may be expected to outnumber wired PC's as early as 2010.. Also, many scenarios for ad hoc networks assume that nodes are potentially mobile.The revolutionary advances in the wireless communication technologies are enabling the realization of a wide range of heterogeneous wireless systems. This technological development is furtherinspiring the researchers to envision several scenarios: Constellation of Wireless Devices (Mobile Ad hoc Networks)[2], Pervasive Systems and Sensor Networks, and Spare Ad hoc Cellular Network**.**A Mobile Ad hoc Network consists of wireless Mobile Nodes (MNs)[3] that cooperatively communicate with each other without the existence of fixed network organization. Reliant on diverse topographical topologies, the MNs are dynamically located and continuously changing their positions.The fast-changing characteristics in ad hoc networks make it difficult to discover routes between MNs.

It becomes important to design efficient and reliable multihop routing protocols to discover[4], organize, and maintain the routes in ad hoc networks. An area where there is much potential for wireless technologies to make a tremendous impact is the area of vehicular ad hoc networks (VANET)[5]. This application has similarities with the ad hoc mesh network for suburban or rural broadband access mentioned earlier. Ubiquitous computing that will pervade society redefining the way in which we live and work.A cell phone is essentially a battery-powered microprocessor[6], with one or more wireless transmitters and receivers optimized for voice I/O. Ready, even when the unexpected happens.It is very important to consider conditions and restrictions created by emergency and catastrophe states. For example, in catastrophe conditions, which duration is unpredictable, saving energy becomes an important goal, as it may be impossible to charge cellular phones[7]. Terrorists may plan their attacks by taking into account the victims' most likely reaction. Therefore, we need protocols that enable quick and efficient delivery of information to people.The source of information could be other users, officials, or generated by sensing devices. Finally, we need ways to guarantee communication and interoperability between the area under disaster and the unaffected areas.Wireless communication is much more difficult to achieve than wired communication because the surrounding environment interacts with the signal, blocking signal alleyways and announcing noise and echoes.There are many features of the wireless medium that distinguish it from other media. The wireless medium is a *shared* medium. This means that unlike wire line systems, where there exist dedicated physical connections between users[8], every user can essentially receive an attenuated version what other users are transmitting[9].Figure 1(a) shows the manner of transmission is *broadcast* of the signal and there is interference in reception of a signal.Another property of a wireless channel is its random time- varying behavior due to the mobility of users and other objects, as well as obstacles in the environment. . More specifically, the channel to a given user might have poor conditions at some times and favorable conditions at other times. This is called the *fading* behavior of the channel. In many situations, multiple copies of the transmitted signal may be received with different delays and different strengths. This is referred to as "multipath fading" and can severely deteriorate the performance when the transmitted signals have shorter duration (e.g broadcate transmission)[10].

Manuscript published on 30 July 2013.
*****Correspondence Author(s)
Islabudeen M, Information Technology, Syed Ammal Engineering College, Ramanathapuram, India.
Sathiya M, Computer Science and Engineering, Syed Ammal Engineering college, Ramanathapuram, India.

© The Authors. Published by Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP). This is an open access article under the CC-BY-NC-ND license http://creativecommons.org/licenses/by-nc-nd/4.0/

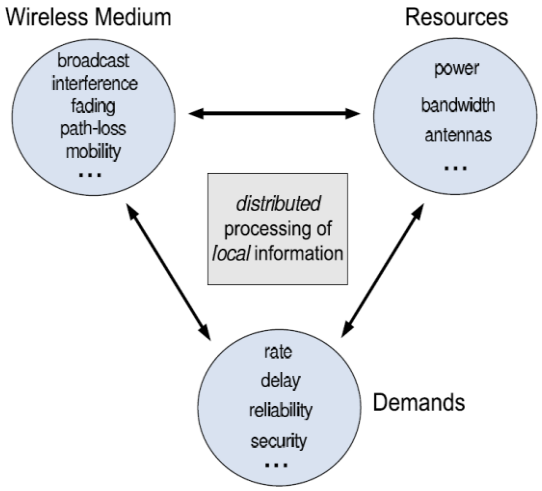

Fig. 1(a) Sources of challenges in analysis and design of wireless networks

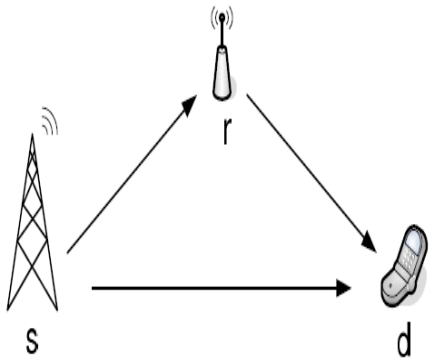

Fig. 1(b) A simple network with one relay component, one source and one destination.

Great interest inexploiting the spatial degrees of freedom in wireless systems by deploying multiple antennas at the transmitter and the receiver. The possibility of using multiple antennas in a network (multi-user) setup has been recently explored.Finding the optimal strategy for the nodes of a network in order to optimally perform a given task is very much an open problem. Consider the simple network, with only three nodes, in the above fig.1(b). The desired task is reliable communication from the source to the destination with the aid of the relay node. The relay node is connected to both the source and destination through communications channels[8]. Even for this simple network, finding the optimal operation at each node for maximizing the rate of reliable communication is unsolved. The main difficulty in a network setup is the distributed nature of the information in the network.

II. PROJECT DESCRIPTION

A. *Project Introduction*

Wireless Local Area Network (WLAN) is popular however, it suffers from all the constraints of wireless networks including low transmit speed and bandwidth, memory and processing power which limits the implementation of security approaches as can be implemented in wired LANs which includes public-key ciphers[1]. Moreover, due to the feature that signals are transmitted in the air, an adversary can easily monitor and intercept all signals. Thus, robust, efficient and effective security measurements are essential for all WLANs. Most of the information now a days is in digital format that can be passed around and injured simply, except it is sheltered. Cryptographic algorithms provide means for protecting the content (encryption) and integrity (hash functions), and verification.The problem with asymmetric key cryptography is that it tends to be much slower than symmetric key cryptography. This can be solved by using public key methods for creating a shared secret that can be used for creating a symmetric key that can further be used for faster ciphering. Diffie-Hellman key exchange, whichis a crucial part of many cryptographic protocols like handshake in Transport layer security (TLS).

B. *Existing System*

WLAN suffers from multiple security holes due primarily to design issues in the decorum itself. One of these issues is the disassociation frame attack[1] in which an attacker injects a management frame that looks as if it originated from the access point. Management frames include information about protocols used as well as control information that need to be transferred from the router to the all-inclusive network. These management packets are disseminated to the network need some encryption. Then every management packet that leaves the AP must be signed with that key.

C. *Proposed System*

Authentication mechanisms are usually needed on top of these key exchange algorithms to handle man-in-the-middle attacks. Fig.2(a) Shows ,Secret key Generation by using original message. This means that a third party might be able to act between the actual parties and learnt the secrets that where not meant for it.The basic transmission unit between wireless transmission is by means of frame. Both stations and access point radiate and gather 802.11 frames when working. Most of frames are data frames containing IP packets, the data.Fig.2(b) shows,original message generated from secret key. Other are management frames and control frame which are used for wireless connection and do not contain data.Disassociation attack is a kind of DoS attack which mainly focuses on destroying the connectivity between station and access point.

Sender Side

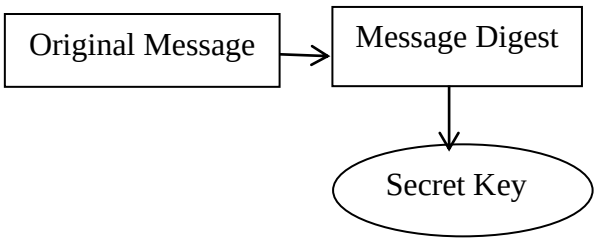

Fig. 2(a) Secret key Generation

Receiver Side

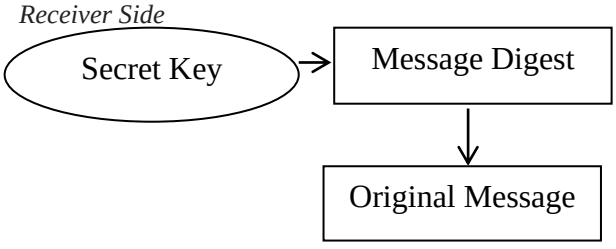

Fig.2(b) Original Message generation From Secret Key

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)
© Copyright: All rights reserved.

III. MODULE DESCRIPTION

A. Architecture Model

The simulation work has been done with The Network Simulator NS2, Version 2.29. In the simulation 100 nodes are randomly distributed within the network field of size 1000m * 1000m. On varying number of nodes in network, going to test the performance of our proposed technique.NS-2 has a companion animation object known as the *Network Animator*, **nam-1**.It is used for visualization of the simulation output and for (limited) graphical configuration of simulation scenarios.Simulation scripts are written in the OTcl language, an leeway of the Tcl scripting language. This construction authorizations simulations to be written and modified in an interpreted environment without having to resort to recompiling the simulator each time a structural change is made.

B. Key Generation

In this key generation module, need to generate a public key and private key for a nodes in a network. With this algorithm we need to find a primitive root of a prime number. Once the primitive root is chosen with that nodes private key we generate a public key for a node.
Choose one prime number q, then primitive root a where a<q.

- Calculate the public key Y_A where $Y_{A=a}{}^{X}{}_{B}$ mod q.
- Calculate the public key Y_B where $Y_{B=a}{}^{X}{}_{A}$ mod q.
- X_A and X_B private keys. .

C. Key Establishment

In Key Establishment module, need to deploy a node with hash key for an efficient secure transmission of packets in the network. The nodes will exchange their public keys and authentication.A hash function is simply an algorithm that takes a string of any length and reduces it to a unique fixed length string. Hashes are used to ensure data and memo reliability, keyword cogency as well as the base of many other cryptographic systems.SHA-1 produces a 160-bit message digest based on principles similar to those used by Ronald L. Rivest of MIT in the design of the MD4 and MD5 message condensation procedures, but has a more traditionalist design.

SHA1 algorithm consists of 6 tasks:
Task 1. Appending Padding Bits. The original message is "padded" (extended) so that its length (in bits) is compatible to 448, modulo 512. The filling rules are:

- The original message is always padded with one bit "1" first.
- Then zero or more bits "0" are padded to bring the length of the message up to 64 bits fewer than a multiple of 512.

Task 2. Appending Length. 64 bits are appended to the end of the padded message to indicate the length of the unique memo in bytes. The guidelines of affixing measurement are:

- The length of the original message in bytes is converted to its binary arrangement of 64 bits. If overspill ensues, only the low-order 64 bits are used.
- Break the 64-bit length into 2 words (32 bits each).
- The low-order word is appended first and followed by the high-order word.

Task 3. Preparing Processing Functions. SHA1 requires 80 processing functions defined as:

- f(t;B,C,D) = (B AND C) OR ((NOT B) AND D)
- f(t;B,C,D) = B XOR C XOR D
- f(t;B,C,D) = (B AND C) OR (B AND D) OR (C AND D)
- f(t;B,C,D) = B XOR C XOR D

Task 4. Preparing Processing Constants. SHA1 entails 80 processing constant words defined as:

- K(t) = 0x5A827999 (0 <= t <= 19)
- K(t) = 0x6ED9EBA1 (20 <= t <= 39)
- K(t) = 0x8F1BBCDC (40 <= t <= 59)
- K(t) = 0xCA62C1D6 (60 <= t <= 79)

Task 5. Initializing Buffers. SHA1 algorithm requires 5 word buffers with the following initial values:

- `H0 = 0x67452301`
- `H1 = 0xEFCDAB89`
- `H2 = 0x98BADCFE`
- `H3 = 0x10325476`
- `H4 = 0xC3D2E1F0`

Task 6. Processing Message in 512-bit Blocks. This is the foremost mission of SHA1 algorithm, which twists over the padded and affixed memo in chunks of 512 bits each. For every contribution chunk, a amount of actions are achieved. This mission can be designated in the subsequent pseudo code slightly modified from the RFC 3174's.

D. Prformance Analysis

Let us focus on the performance of this routing protocol. We evaluated the performance using NS2. Analyzing the performance of our encryption technique based on End to end delay, Packet Lost, Throughput and Packet
Delivery Ratio.

Packet Lost Ratio

When our Internet link is unhurried, it may be the effect of wallet harm. Deliberate your wallet harm percentage will help you determine if the slowness issue is based on your connection to the Internet, or it trunks from a dissimilar delinquent. Meager Internet links can be produced by a amount of details, so using a wallet harm percentage formula is a part of the troubleshooting process. If the outcomes show a great wallet harm, commerce the support division of your Internet provider.
Packet lost = Number of packet send – Number of packet received .
The lower value of the packet lost means the better performance of the protocol.

Packet Delivery Ratio

The ratio of the number of delivered data packet to the destination. This demonstrates the smooth of delivered data to the destination.
Packet Delivery Ratio=∑ Number of packet receive / ∑ Number of packet send
The superior rate of wallet delivery percentage means the better performance of the protocol.

End-to-end Delay

The average time taken by a data packet to arrive in the destination. It also contains the suspension produced by route discovery process and the queue in data wallet transmission. Only the facts packets that successfully delivered to destinations that counted.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)
© Copyright: All rights reserved.

End to End Delay=∑ (arrive time – send time) / ∑ Number of connections

The lesser rate of end to end delay means the better performance of the protocol.

Throughput

It is the average rate of successful message delivery over a communiqué network. This facts may be delivered over a corporeal or rational connection, or permit over a certain network node. The throughput is generally unhurried in bits per second (bit/s or bps), and occasionally in data packets per second or facts packets per time slot.

The higher value of throughput means the better performance of the protocol

III. FLOW DIAGRAM

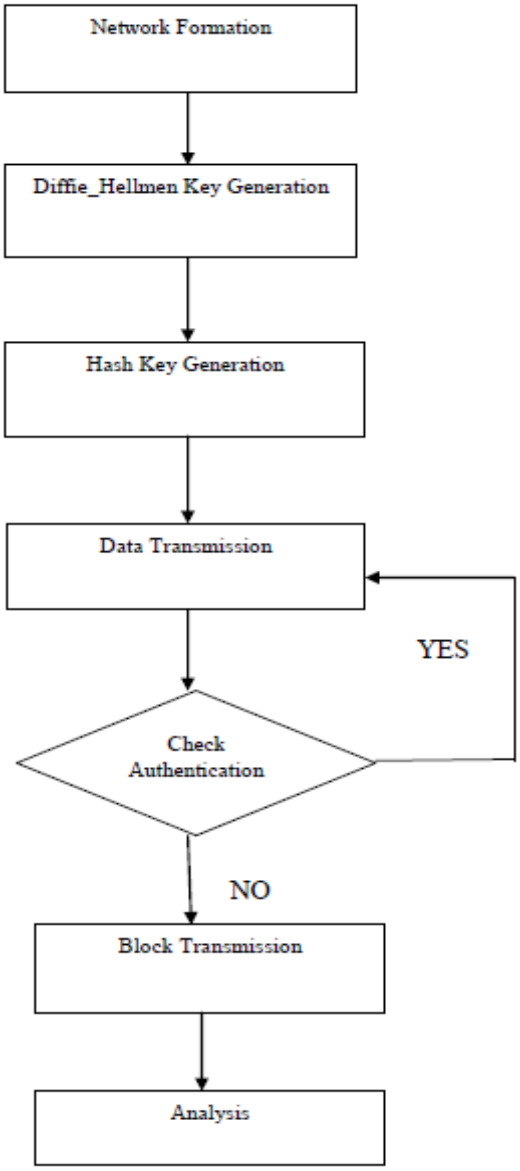

Fig. 4 Flow Diagram

Fig.4 shows flow of processing ,it start with architecture model designed with NS2 simulation tool.Node position,node color,node distance defined by using NS2 tool.In key generation module for each node private key and public key been generated.In key establishment module secret key is generated for each node by using SHA algorithm.In performance analysis module analyse throughput,end to end delay,packet delivery ratio,packet harm.

IV. COMPARISON

Table 1
Existing System Vs Proposed System

Calculation	Existing	Proposed
Packet Delivery Ratio	97	98
Throughput	3.5	5
Lost	16	8
End to End delay	0.2	0.16

Table 1 describes comparison between existing system and proposed system,it achieve high performance than existing system.

V. CONCLUSION AND FUTURE ENHANCEMENT

In this paper, We presented a diffie-hellman triple key method for securing the management frames, which hackers use to de-authenticate all users in a network. Use an efficient encryption algorithm for securing management frames by symmetric key process. Also as compared with the existing algorithms our diffie-hellman triple key method showed good performance in the simulation results.As for some contexts we should be good to keep the key sizes relatively small. In future can modify our proposed diffie-hellman triple key method to reduced key size.

REFERENCES

1. Mohammad S. Obaidat, Fellow, IEEE, and Tari Guelzim,"ACounterDisassociation Mechanism (CDM) for Wireless LANs and its Performance Simulation Analysis,"IEEE SYSTEMS JOURNAL, VOL. 4, NO. 1, MARCH 2010.
2. T. Guelzim and M. S. Obaidat, "A novel neurocomputing based scheme to authenticate WLAN users employing distance proximity threshold,"in Proc. IEEE Int. Conf. Security and Cryptography, SCRYPT, Porto,Portugal, pp. 145–153, Jul. 2008.
3. M. S. Obaidat and N. Boudriga, Security of e-Systems and ComputerNetworks. Cambridge, U.K.: Cambridge Univ. Press, 2007.
4. J.-C. Lin, Y.-H. Kao, and C.-W. Yang, "Secure enhanced wireless transfer protocol," in Proc. 1st Int. Conf. Availability, Reliability andSecurity (ARES'06), pp. 536–543,Apr. 2006.
5. X.Wang, Y. L. Yin, and H. Yu, "Finding collisions in the full SHA-1,"CRYPTO 2005.
6. S. Michelle and Srinivasan, "State based key hop protocol: A lightweight security protocol for wireless networks," in Proc. 1st ACM Int.Workshop on Performance Evaluation of Wireless Ad Hoc, Sensor, andUbiquitous Networks, pp. 112–118,Oct. 2004.
7. C. He and J. C. Mitchell, "Analysis of the 802.11i 4-way handshake,"in ACM Workshop on Wireless Security, pp. 43–50,Oct. 2004.
8. P. Nicopolitidis, M. S. Obaidat, G. Papadimitriou, and A. S.Pomportsis Wireless Networks. New York: Wiley, 2003.
9. J. Bellardo and S. Savage, "802.11 Denial-of-service attacks: Real vulnerabilities and practical solutions," in Proc. USENIX Security Symp.,pp. 15–28.,Aug. 2003.
10. J. Li and W. Jia, "Traffic analysis ad hoc networks based on location-aware clustering," in Proc. 23rd Int. Conf. Distributed Computing Systems Workshops (ICDCSW'03), 2003.

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)
© Copyright: All rights reserved.