ISSN (Online) : 2319 – 8753
ISSN (Print) : 2347 - 6710

IJIRSET

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization, Volume 3, Special Issue 1, February 2014

International Conference on Engineering Technology and Science-(ICETS'14)

On 10th & 11th February Organized by

Department of CIVIL, CSE, ECE, EEE, MECHNICAL Engg. and S&H of Muthayammal College of Engineering, Rasipuram, Tamilnadu, India

A Secure Approach with Physical Layer Encryption in MANET

C. Suhashini[1], S. Sivakumar[2]

Department of CSE, Adhiparasakthi Engineering College, Melmaruvathur, Tamilnadu, India. [1, 2]

Abstract — Establishing correct and efficient routes is an important design issue in mobile ad hoc networks (MANETs), a more challenging goal is to provide secured routing, because ad hoc environment is accessible to both legitimate network users and malicious attackers. Moreover, as the wireless links are highly error prone and providing security is still a critical task. Generally, security in this type of network is provided by interference of signals, which is not energy efficient. Physical layer security has been considered to provide confidentiality against eavesdropping. Shift difference algorithm has been proposed to transfer the data securely over the network. It converts the data into noise for transmission. Network traffic has been reduced, as only intended participants transmit the data. By default network layer security has been provided by encryption.

Keywords — physical layer security, eavesdropping,network layer security.

I. INTRODUCTION

Wireless networks are usually vulnerable to attacks by intruders of various nature, and there is no doubt that including security issues in the system design would be very desirable. One approach to security issues focuses on the physical layer [1]. Focusing on transmission-only problems, instead of detection ones. This problem can be traced back to the seminal 1975 work by Wyner [2] on the wiretap channel, where the tradeoff between the communication rate achievable by the legitimate user and the amount of information intercepted by the wiretapper, as measured in terms of equivocation, is addressed. Obviously, Wyner's viewpoint was not focused on modern wireless networks and results form a solid basis for the modern approach to physical-layer security [3]–[8] and later generalized by Csiz´ar and K¨orner [9]. The wiretap channel assumes that the legitimate receiver has a better channel than the eavesdropper. For this reason, researchers have long considered that, in many wireless communication scenarios, the wiretap channel is impractical. various physical-layer techniques were proposed to achieve secure communication, even if the receiver's channel is worse than the eavesdropper's channel.

One of the main techniques is the use of interference or artificial noise to confuse the eavesdropper. With two base stations connected by a high-capacity backbone, one base station can simultaneously transmit an interfering signal to secure the uplink communication for the other base station [10], [11]. In the scenario where the transmitter has a helping interferer or a relay node, the secrecy level can also be increased by having the interferer [12] or relay [13] to send code words independent of the source message at an appropriate rate.

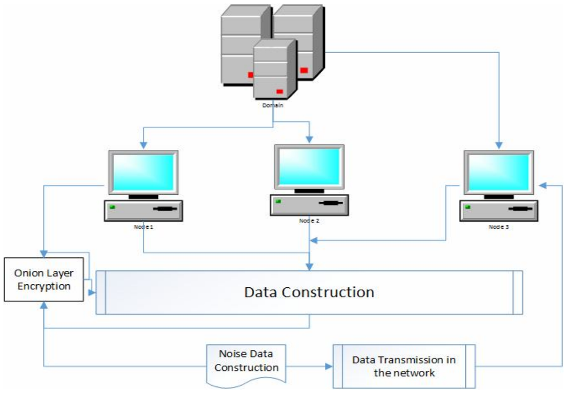

Figure 1 Architecture diagram for physical layer encryption

A. Unique Features of MANET

The following are the features of MANET by which it varies from other types of network.

Human interface: with device Screens and keyboards tend to be small, which may make them hard to use. Alternate input methods such as speech or handwriting recognition require training.

Security standards: When working mobile, one is dependent on public networks, requiring careful use of VPN (Virtual private Network). Security is a major concern while concerning the mobile computing standards on the fleet. One can easily attack the VPN through a huge number of networks interconnected through the line.

Power consumption: When a power outlet or portable generator is not available, mobile computers must rely entirely on battery power. Combined with the compact size of many mobile devices, this often means unusually expensive.

Transmission interferences: Weather, terrain, and the range from the nearest signal point can all interfere with signal reception. Reception in tunnels, some buildings, and rural areas is often poor.

Distributed operation: There is no background network for the central control of the network operations; the control of the network is distributed among the nodes. The nodes involved in a MANET should cooperate with each other and communicate among themselves and each node acts as a relay as needed, to implement specific functions such as routing and security. Multi hop routing: When a node tries to send information to other nodes which is out of its communication range, the packet should be forwarded via one or more intermediate nodes.

Autonomous terminal: In MANET, each mobile node is an independent node, which could function as both a host and a router.

Dynamic topology: Nodes are free to move arbitrarily with different speeds; thus, the network topology may change randomly and at unpredictable time. The nodes in the MANET dynamically establish routing among themselves as they travel around, establishing their own network.

Light-weight terminals: In maximum cases, the nodes at MANET are mobile with less CPU capability, low power storage and small memory size.

Shared Physical Medium: The wireless communication medium is accessible to any entity with the appropriate equipment and adequate resources. Accordingly, access to the channel cannot be restricted.

II.BACKGROUND AND RELATED WORK

This section introduces some background knowledge including the network Architecture and some related works.

A. ENERGY EFFCIENCY

MANETs, therefore, impose a very fundamental constraint on the security solution being designed for this environment, i.e. "the security solution needs to be highly efficient in energy consumption", and it translates to the following requirements:

Minimum Control Overhead: Control overhead (bytes or packets) of the routing protocol needs to be minimized. Lower the control overhead, higher is the channel bandwidth utilization due to minimizing the transmission of redundant control bytes. Moreover, lower energy would be required to actually transmit and/or receive bits at the network interface card.

Minimum Computational Complexity: An algorithm with lower computational load allows the mobile node to achieve longer battery life by consuming less amount of energy for its internal processing.

Energy efficient routing requires optimizing the packet routing process for lower energy consumption. However, none of the classical MANET routing algorithms have been designed keeping in view energy efficiency. The authors in [9] studied DSR and AODV for energy efficiency and report that protocol design parameters, such as lower delay and higher packet delivery ratio, do not achieve low energy consumption.

B. Related Work

The popularity of MANETs has lead to an increasing interest in addressing their security issues. There are a number of proposals for secure MANETs that are based on standard cryptography and Artificial Immune Systems (AISs). The cryptographic systems include both the symmetric as well as asymmetric approaches. The AODV protocol has been secured by a public key system (using asymmetric keys) through Secure Ad-Hoc On-demand Distance Vector protocol (SAODV) [15]. While the DSR protocol has a secure version ARIADNE [16], which employs symmetric key cryptography to provide security to the source routing process. However, cryptography includes compute intensive mathematical operations [17], especially the asymmetric systems, and thus imposes heavy computational load on mobile nodes causing rapid battery depletion. Moreover, most of these security systems involve computing digital signatures and/or message hashes and transmitting them along with the data, resulting in transmission of additional control information, which reduces the effective protocol throughput.

C.SECURITY GOALS

In MANET, all networking functions such as routing and packet forwarding, are performed by nodes themselves in a self-organizing manner. For these reasons, securing a mobile ad -hoc network is very challenging. The goals to evaluate if mobile ad-hoc network is secure or not are as follows: Availability: Availability means the assets are accessible to authorized parties at appropriate times. Availability applies both to data and to services. It ensures the survivability of network service despite denial of service attack. Confidentiality: Confidentiality ensures that computer-related assets are accessed only by authorized parties. Protection of information which is exchanging through a MANET. It should be protected against any disclosure attack like eavesdropping- unauthorized reading of message.

Integrity: Integrity means that assets can be modified only by authorized parties or only in authorized way.. Integrity assures that a message being transferred is never corrupted. Authentication: Authentication is essentially assurance that participants in communication are authenticated and not impersonators. The recourses of network should be accessed by the authenticated nodes.

Authorization: This property assigns different access rights to different types of users. For example a network management can be performed by network administrator only.

Resilience to attacks: It is required to sustain the network functionalities when a portion of nodes is compromised or destroyed.

Freshness: It ensures that malicious node does not resend previously captured packets.

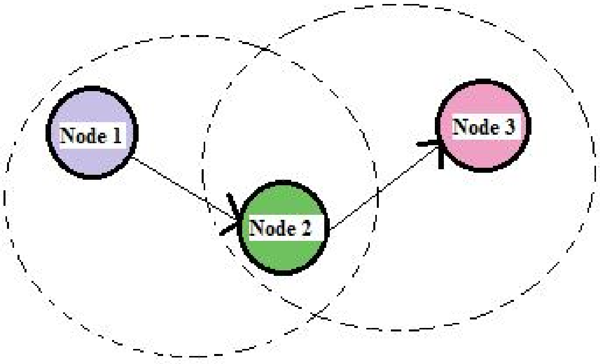

Figure 2 MANET Architecture

III. ALGORITHM

A. TRIPLE DATA ENCRYPTION STANDARD

In cryptography, Triple DES is the common name for the Triple Data Encryption Algorithm (TDEA or Triple DEA) block cipher, which applies the Data Encryption Standard (DES) cipher algorithm three times to each data block.

The original DES cipher's key size of 56 bits was generally sufficient when that algorithm was designed, but the availability of increasing computational power made brute-force attacks feasible. Triple DES provides a relatively simple method of increasing the key size of DES to protect against such attacks, without the need to design a completely new block cipher algorithm. Triple DES uses a "key bundle" which comprises three DES keys, K1, K2 and K3, each of 56 bits (excluding parity bits).

Ciphertext = EK3 (DK2 (EK1 (plaintext)))

DES encrypts with K1, DES decrypt with K2, then DES encrypt with K3.

Plaintext = DK1 (EK2 (DK3 (ciphertext)))

Each triple encryption encrypts one block of 64 bits of data.

In each case the middle operation is the reverse of the first and last. This improves the strength of the algorithm when using keying option 2, and provides backward compatibility with DES with keying option 3.

Keying option 1: All three keys are independent.

Keying option 2: K1 and K2 are independent and K3 = K1.

Keying option 3: All three keys are identical, K1 = K2 = K3.

Keying option 1 is the strongest, with 3 × 56 = 168 independent key bits.

Keying option 2 provides less security, with 2 × 56 = 112 key bits. This option is stronger than simply DES encrypting twice, e.g. with K1 and K2, because it protects against meet-in-the-middle attacks.

Keying option 3 is equivalent to DES, with only 56 key bits. This option provides backward compatibility with DES, because the first and second DES operations cancel out. It is no longer recommended by the National Institute of Standards and Technology (NIST) and is not supported by ISO/IEC 18033-3.

Each DES key is nominally stored or transmitted as 8 bytes, each of odd parity, so a key bundle requires 24, 16 or 8 bytes, for keying option 1, 2 or 3 respectively.

Algorithm TRIPLE DES Algorithm for secret key generation

```
 uint state [2], idx, t;
 IP (state, in);
 (Idx=0; idx < 15; ++idx)
{t = state [1];
 State [1] = f (state[1],key[idx]) ^ state[0];
 State [0] = t;
  }
 State [0] = f (state[1],key[15]) ^ state[0];
```

```
  InvIP(state,out);
}
three_des_key_schedule (uchar key [], uchar schedule
[][16][6], uint mode)
{
  if (mode == ENCRYPT) {
   Key schedule (&key [0], schedule [0], mode);
   Key schedule (&key [8], schedule [1],!mode);
   Key schedule (&key [16], schedule[2],mode);
  }
  else {
     Key schedule (&key [16],schedule[0],mode);
     Key schedule (&key [8],schedule[1],!mode);
     Key schedule (&key [0],schedule[2],mode);
  }
}
three_des_crypt (uchar in[], uchar out[], uchar key[][16][6])
{
    des_crypt (in, out, key [0]);
  des_crypt (out, out, key [1]);
  des_crypt(out, out,key[2]);
}
```

B. SHIFT DIFFERENCE ALGORITHM

Due to the increase in business transactions in the internet. There is a need for safety data transmission. There exists a threat to the message that we transmit using old known encryption algorithms, because it is known public to all. Hence we introduce a new algorithm for safety data transmission.

Read the first character of the file and use this as key for subsequent characters. Find the difference (D) for the successive characters and write the difference in the cipher text file.

If D=+ve, write the D value as such.

If D=-ve, we use a filler character and the D value.

The filler character is a prime number. The key is shifted either as left shift or right shift on the cipher text, based on number of bits. Hence the key on the cipher text is even changed which provides the strong security. For decryption Reverse shift to the shift that done on the Encryption side to Obtain the Key. The key Obtained will be used for the generation of the plain text. The algorithm is simple and secure, because the key is not intelligible to the hacker. The encrypted text is independent of language. Shifting numbers is an Prime Number, hence it is difficult to identify.

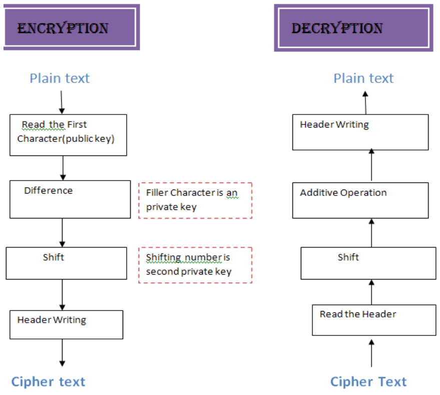

Figure 3 Shift Difference Algorithm Process

IV. CONCLUSION

A simple application is created for secure data transaction in mobile ad hoc network. Physical layer security is considered to provide confidentiality against eavesdropping. Physical layer encryption has been provided, by encrypting the data before being transmitted in the network. Network layer

security is provided as default. Physical layer security has been provided by transmitting data as noise over the network. An enhancement to this application can be considered to provide physical layer encryption, while transmitting data from multiple source to single destination and from multiple source to multiple destination.

REFERENCES

[1] H. V. Poor, "Physical layer security in wireless networks: Some recent results," presented at the Communication Theory Workshop (CTW), St. Croix, U.S. Virgin Islands, May 11–14, 2008.

[2] A. D. Wyner, "The wire-tap channel," AT&T Bell Labs Tech. J., vol. 54, no. 8, pp. 1355–1387, Oct. 1975.

[3] I. Csiszár and J. Korner, "Broadcast channels with confidential messages," IEEE Trans. Inf. Theory, vol. 24, no. 3, pp. 339–348, May 1978.

[4] Y. Liang, H. V. Poor, and S. Shamai (Shitz), "Secrecy capacity region of parallel broadcast channels," in Proc. Information Theory Applications Workshop, Nice, France, Jan. 29–Feb. 2 2007, pp. 245–250.

[5] Y. Liang, H. V. Poor, and S. Shamai (Shitz), "Secure communication over fading channels," IEEE Trans. Inf. Theory, vol. 54, no. 6, pp. 2470–2492, Jun. 2008.

[6] Y. Liang and H. V. Poor, "Multiple-access channels with confidential messages," IEEE Trans. Inf. Theory, vol. 54, no. 3, pp. 976–1002, Mar. 2008.

[7] Z. Li, W. Xu, R. Miller, and W. Trappe, "Securing wireless systems via lower layer enforcements," in Proc. 2006 ACM Workshop Wireless Security, Los Angeles, CA, 2006, pp. 33–42.

[8] M. Bloch, J. Barros, M. R. D. Rodrigues, and S. W. McLaughlin, “Wireless information-theoretic security,” IEEE Trans. Inf. Theory, vol. 54, no. 6, pp. 2515–2534, Jun. 2008.

[9] I. Csisz´ar and J. K¨orner, “Broadcast channels with confidential messages,” IEEE Trans. Inf. Theory, vol. 24, no. 3, pp. 339–348, May 1978.

[10] M. L. Jorgensen, B. R. Yanakiev, F. E. Kirkelund, P. Popovski, H. Yomo, and T. Larsen, “Shout to secure: Physical-layer wireless security with known interference,” in Proc. IEEE GLOBECOM, Washington, DC, Nov. 2007, pp. 33–38. 3842 IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY, VOL. 59, NO. 8, OCTOBER 2010.

[11] O. Simeone and P. Popovski, “Secure communications via cooperating base stations,” IEEE Commun. Lett., vol. 12, no. 3, pp. 188–190, Mar. 2008.

[12] X. Tang, R. Liu, P. Spasojevic, and H. V. Poor, “Interference-assisted secret communication,” in Proc. IEEE ITW, Porto, Portugal, May 2008, pp. 164–168.

[13] L. Lai and H. E. Gamal, “The relay-eavesdropper channel: Cooperation for secrecy,” IEEE Trans. Inf. Theory, vol. 54, no. 9, pp. 4005–4019, Sep. 2008.

[14] Laura, M. F.; Mobile Networks and Applications, 6(3) (2001), 239–249.

[15] Zapata, M. G.; Internet-Draft, draft-guerrero-manet saodv-05.txt, February, 2005.

[16] Yih-Chun, H., Adrian, P. and David, B. J.; Wireless Networks, 11(1-2)(2005), 21–38.

[17] Stallings, W.; Cryptography and Network Security - Principles and Practices, Pearson Educ. Inc., 2003.