KEY GENERATION FRAMEWORK FOR MULTIPLE WIRELESS DEVICES USING MULTIPATH ROUTING

Vijayaganesh M , Fungkha Narzary, and Rajanand S

Veltech Hightech Chennai-62, India,

ABSTRACT

The secret key generation for wireless devices, use for observing with every devices such as signal strength and range of their distance achieved by lower bit matching via RSS. In previous system they are defined secret key for multiple devices from one centralised device. Signal strength will be varied for each devices and connection of that devices also will be lose when the devices goes out of the range. In recent years network security become important issue. Data can be shared with other devices using secret key. We have designed and implement multiple key generation for multiple devices. Each time generated a new secret key for making communication with other devices. Overcome the range of signal strength and centralised networks, able to communicate with any devices with help of AES. Expand the key strength and create a different secret key upto 256 bit.

KEYWORDS

Secret key generation, group communication, expending key strength

1 .INTRODUCTION

Observe the outputs of distinct albeit correlated sources, could devise a secret key by means of public communication. In other words, these terminals are able to generate common randomness regarding which an eavesdropper, with access to this communication and perhaps also to side information comprising the outputs of other sources which are correlate with the previous sources, can glean only negligibly small amount of mutual information.

Today world come up with mobile environment. Use the mobile for communication, distance identify and gather the information. We are present security during accessing the data via wireless devices. Hearing of terms such as telecommuting enables anyone to work from home, at the same time accessing resources also. The importance of computers, laptop, and smart phones, has in turn made wireless devices. The portability of the devices are enable user to access all services as if they were in the internal network of their company. For example, the use of tablets pc and I pads. This new technology enables users to modify documents, use of internet, accessing e-mail, download files, take photographs and also support video and voice conferencing.

Secret key generate secure communication between two communication devices and given security to data's. Now multiple technologies are came with help of secret key concept. Most of research depends on the received signal, including that theoretical analysis. Other than the recent work that was performed in home based devices., there is very little research on evaluating how effective RSS based work extraction is in real environments under real settings. Proposed scheme address this important limitation of the existing research in this paper with the help of wide scale real life measurements in both static and dynamic environments.

DOI : 10.14810/ecij.2015.4102

Secure wireless communications is a challenging problem due to the share data between devices. Most existing security protocols apply encryption and decryption techniques for bit scrambling at the application layer by exploiting a shared secret key between pairs of communicating nodes. Secure keys are distinct for distinct pair wise links with a probability that the two users sharing a common link generate the same key [5].Security techniques that exploit the randomness of wireless channels for getting the secret key by performing encryption and decryption. Focus on pair wise key generation, its highly scalable and improve the key bit generation rate by a couple of orders [6].

In pair-wise independent network, every pair of terminals observes a common pair-wise source that is independent of all sources accessible to the other pairs[15]. Here three specific problems are investigated. One was each terminals are in observations with the others. All these terminals wish to generate a common secret key. Two was designated terminals wish to generate a secret key with the help of other terminals. Three was all the terminals wish to generate a common secret key.

The communicating parties require some shared secret key with which to encrypt the message so that it cannot be understood by an enemy observer. The exchange of some information between the parties is necessary to achieve the bounds and various information [24]. Two cars to extract a secret key from RSSI values in such a way that nearby cars cannot obtain the same secret[30]. The main contribution of this work is to group of the physical channel characteristics with key generation algorithms to secure wireless networks.

2 .RELATED WORK

In previous research are shared the secret keys to de vices and compare their lower bit mapping [13], they are using pin model. In a typical multipath environment, the wireless channel between each pair of terminal produces a random mapping between the transmitted and received signals which is time-varying and location specific.

The novel methodologies which allow robust secret key extraction from radio channel measurements which user from real world non-reciprocities a prior unknown fading. The fading signal are verified with their neighbour devices.The secret key generation utilizing physical layer information of the radio channel it allows any two wireless devices within transmission range of each other to extract a share symmetric cryptographic key while does not require a fixed data range and destination range among the devices [1]. Based on the principle of two wireless devices can interact with secret bits independently by using the sampled sequence from the radio channel between them within the coherence time of the channel. Unlike existing key generation algorithms, such as Diffie-Hellman, which deals the secret key generation between pair of devices. It's provided by the temporal and spatial variation of the radio channel can achieve information theoretical secrecy [4]. We place our work in the context of relate research in section II. We provide a feasibility study of using fine-grained channel response information for secret key extraction and present the attack model in section III. We present the proposed channel gain complement assisted key generation and extraction in section IV. Comparison and simulation results based on performance of secret key using AES as given in section V.

3 . ARCHITECTURE

From the architecture diagram its shows multiple devices with unique secret key generation. There many devices are need to access the data. It require secret key to access data so they send request to key generator. Key generators observe the devices based on the RSS signal and encrypt

the keys send to device which is sent the request. Devices are get the unique keys after decrypt the key which are send by key generator by using AES algorithm, Key length 128bit so it's little faster than previous system. Allows the devices to access the data by extract the secret keys via communication channel.

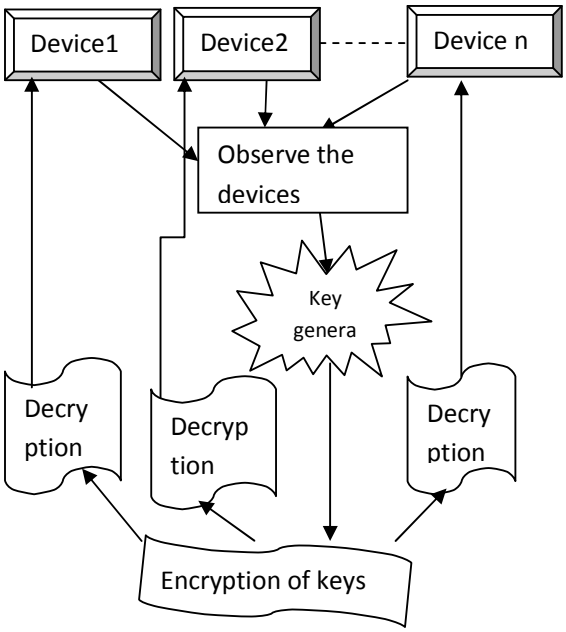

Figure1. Architecture Diagram

4. METHODOLOGY

The challenges arising from utilizing RSS measurements for group key generation. First, the RSS values obtain between a pair of devices cannot be securely passed to other devices making it hard to reach key agreement among multiple devices without the availability of a particular range. Second, due to the multiple of mobile devices, the devices within the group that need to establish a secret key may not be within each other's communication range, making the existing RSS-based methods not applicable. To address these challenges, we define AES algorithm. Our frameworks consist of random number generation and key authentication..

Algorithm:

For i=1 to n do
$K_{i=}K_{i-1+}R_i$
Where |Pi|=128
$X_i=P_i+C_i$
$T=HASH(X_1||X_2||\ldots\ldots\ldots X_n)$
Where $C=C_1||C_2||\ldots\ldots..C_n$

Let's say P_i denotes the plaintext block, where 1<i<n, and n is total no of blocks.

Key Expansion (byte key[16],word w[44])
Step 1:For i=0 to 4 do
Step 2:W[i]= key[4*i],key[4*i+1],key[4*i+2],
key[4*i+3]

Step 3:For i=4 to 44 do
Step 4:T=w[i-1]
Step 5:If i|4 =0
Step6:T=subword * rotword (T)+rcon[i/4]
Step 7:W[i]-w[i-4]=T;

The key is divided by four parts of encryption and decryption then expanded key W[i] depends on the immediate preceeding word, w[i-1] and the word four positions back w[i-4].

Rotword-is a one byte word. This was transformed the input word.

Subword-submit the input word

We now turn to a discussion of each of the four transformations used in AES. For each stage, we mention the forward (encryption) algorithm, the inverse (decryption) algorithm, and the rational for the design of that stage. Design of that secret key between inputs bits and output bits, bits rate compared and mapped each other. A device can communicate with any other devices which are connected in the network.

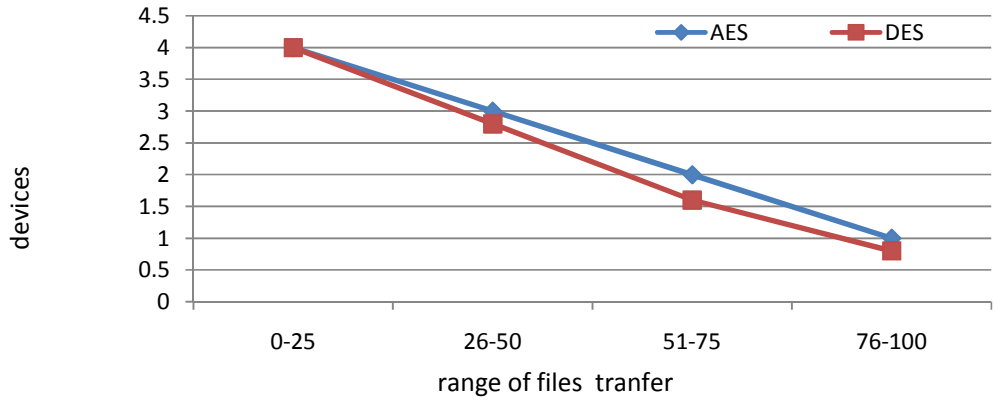

Figure2. Comparison of devices and its range due to transfer the data

Compare the devices and their data transferring rate, comparison of four devices it allows different various speed. If data sizes are increases than speed of devices will become low. Numbers of devices are no problem.

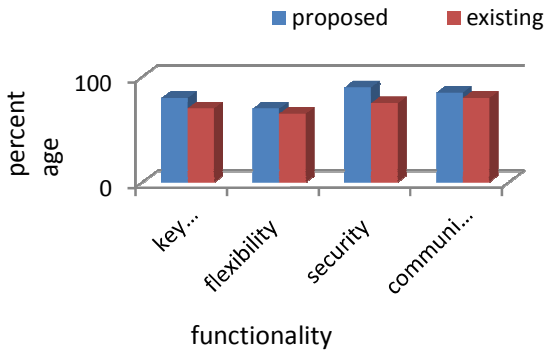

Figure3. Comparison existing and proposed

Compare the secret key generation its efficient than other previous research because its generate 128 bit key. Flexibility to changes of keys. Different unique key provide each time so security will be efficient. communication speed depends on file size

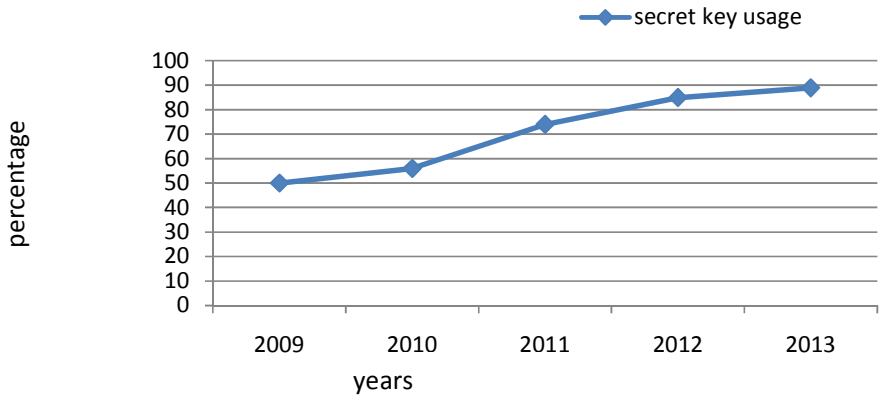

Figure4. Usage percentage of secret keys

5 .PERFORMANCE ANALYSIS

Compare the secret key generation and its usage performance between DES and AES. DES was older one compare with AES. Due to performing the encryption and decryption DES takes 16 rounds, but AES takes 10 rounds only. So AES generate secret key as faster and efficient.

Factors	**AES**	**DES**
Developed	2000	1977
Key size	128 to 256 bits	56 bits
Block size	128 bits	64bits
Cipher & decipher	Use same key	Use same key
Encryption	Faster	Moderate
Decryption	Faster	Moderate
Security	Excellent secured	Not secure enough
Rounds	10	16

Table1.comparison of AES and DES

Based upon the secret key generation AES can generate key as fastly and length of key also bigger than DES. AES key length start from 128bits up to 256bits and it divides the block size as 128bits. AES one of the symmetric key cryptographic algorithm so uses the same key for both encryption and decryption. Compare the security level also AES gives excellent security to data via its secret key. Key length is higher so every time generate distinct key easily. AES can able to generates millions of unique secret keys. Due to generation of key it takes 10 rounds then reduce the time and increase the key length.

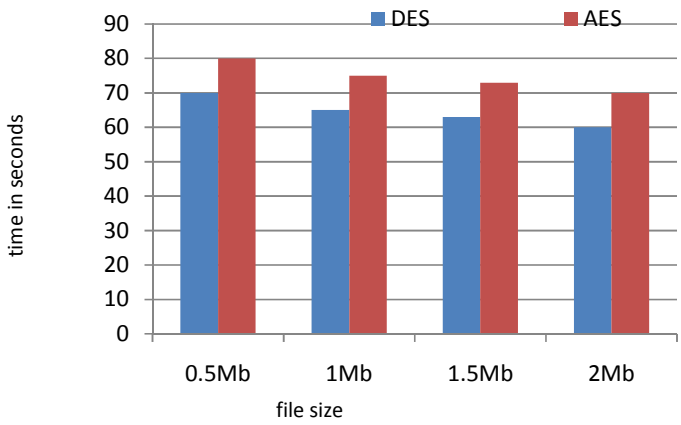

Figure5. Comparison of time taken

A number of files in different sizes were showed into the simulation test. From the comparative study all possible factors can possible to print secret keys as fast and secure.

Comparing the security level our secret key generation is very secure than existing. The key length taken up to 256 bits. so it can generate the millions of different keys, key length was another one important advantage here not easy to judge the key . This can provide the more security to data and increase the hardware and software performances.

6.CONCLUSION

Secret key designed and group secret key generation for multiple wireless devices. The scheme take an advantages of provides different key for each action performance. We given the solution for access the data from anywhere it's no need range of wireless device. Key length has been expanded A result from implementation of secret key is faster than DES with help of using AES algorithm.

REFERENCES

[1] B. Azimi sadjadi, A. Kiayias, A. Mercado, and B.Yener, "Robust key generation from signal envelopes in wireless networks" , in ACM CCS, pp. 401-410(2007).

[2] A. sayeed and A. Perrig, "secure wireless communications: Secret keys through multipath", in IEEE ICASSP,pp.3013-3016.0(2008).

[3] Q. Wang, H. Su, K. Ren and K. Kim, "Fast and scalable secret key generation exploiting channel phase randomness in wireless networks", in IEEE INFOCOM, (2011).

[4] N.Patwari, J. Croft, S. Jana and S. Kasera, "High rate uncorrelated bit extraction for shared secret key generation from channel measurements", IEEE Transactions on mobile computing, pp, 17-30(2009).

[5] J.Croft, N. Patwari, and S. Kasera, "Robust uncorrelated bit extraction methodologies for wireless sensors", in ACM/IEEE ICNP, pp, 70-81(2010).

[6] Y. Kim, A. Perrig and G.Tsudik, "Tree- based group key agreement", TISSEC(2004).

[7] S. Nitinawarat, C. Ye, A. Barg, P. Narayan, and A. Reznik, "Secret key generation for a pair wise independent network model, "IEEE TIFS, vol.2, no.3, pp. 364-375(2007).

[8] S.Nitinawarat and P. Narayanan, "Perfect omniscience, perfect secrecy, and steiner tree packing," IEEE Transactions on information Theory(2010).

[9] C. Ye and A. Reznik, "Group secret key generation algorithms," in IEEE ISIT(2007).

[10] R. Wilson, D. Tse, and R. Scholtz, "Channel identification" Secret sharing using reciprocity in ultrawideband channels," IEEE TIFS, vol.2, no.3, pp.364-375(2007).
[11] Z. Li, W. Xu, R. Miller and W. Trappe, "Securing wireless systems via lower layer enforcements," in Proceeings of the 5th ACM workshop on Wireless security, pp.33-42(2006).
[12] I. Csiszar and R. Ahlswede, "secrecy capacities for multiple terminals,"IEEE Transactions on Information Theory , vol. 50,pp. 3046-3061, (2004).
[13] H. Liu, J. Yang, and Y.Chen, "Collaborative secret key extraction leveraging received signal strength in mobile wireless networks, " in IEEE INFOCOM, pp. 927-935(2012).
[14] O. Arazi and H.Qi,"Self-certified group key generation for ad hoc clusters in wireless networks," in IEEE INFOCOM(2005).
[15] U. Maurer and S. Wolf,"Secret key agreement over a non authenticate chanel part iii,"IEEE Transactions on Information Theory, vol.49,pp.822-851(2003).