I J C T A, 9(16), 2016, pp. 7879-7883

Secure Communication Over Untrusted Relay

S. Ushasukhanya[1], A. Nithyakalyani[2], S. Girija[3], T.Y.J. Naga Malleswari[4], Rupendra[5] and Harshitha[6]

ABSTRACT

In this paper, a combination of computer hardware, cabling, network devices, and computer software was used together to allow computers to communicate with each other. The aim of any computer network is to enable multiple computers to communicate. Data will be secured while transmitting through trusted relay and it does not require any secret key between them.The main drawback in trusted relay is that there will be a data loss when multiple data are sent, hence reducing the efficiency. In this paper, focus on a technique for the transmission of data through a untrusted relay, where the communication takes place between the nodes and the antennas thereby introducing the key generation scheme where we can send our desired data to the desired node without being revealed. This is achieved by the concept of zero forcing and minimum mean square error channel estimators for non-partially, and fully colluding modes of untrusted relays.

Keywords: Transmission through untrusted relay, Salt algorithm, RC4 algorithm, SKR

1. INTRODUCTION

Recently security for wireless communications at physical layer has attracted considerable attention. A lot of work focuses on establishing private communication links without using a secret key. These schemes are designed to obtain a positive secrecy rate without using any pre-shared key between two legitimate nodes. However, it is not guaranteed that such a scheme is always feasible. As another approach to physical-layer security, the secret key generation has been researched, that exploits the randomness and the reciprocity of the wireless channels to generate a secret key. The physical-layer secret key generation has been proposed mainly for a direct communication link between legitimate transmitter and receiver. In case, the direct connection channel cannot be good enough to generate a key, we can consider the relaying/cooperative scenario. A three time- slot key generation scheme for two single antenna legitimate nodes with the help of a relay has been proposed. The salt algorithm is used for password protection added to the hash to prevent a collision by uniquely identifying a user's password, even if another user in the system has selected the same password. The transmission of data is done securely through untrusted relay using RC4 algorithm for encryption and decryption. A key generation scheme exploiting two-way relaying has been proposed, and the secret key rate (SKR) has been presented using the k-nearest neighbor distance mutual information estimation. In fact, most prior works of key generation with relaying channels considered only trusted relays. However, nodes even in the same network may have different levels of security clearance. For instance, they can have varying levels of access to certain information although they are operating with agreed protocols and serving as relays. Therefore, the key generation in the presence of untrusted relays should be investigated. As an effort to generate a secret key with untrusted relays, a scheme with multiple relays has been proposed. In this work, the scheme makes each relay broadcast an XORed version of two

[1,2,3,4] Department of Computer Science Engineering, SRM University, Chennai, *Emails: ushasukhanya.s, nithyakalyani.a, girija.s, nagamalleswari.t @ktr.srmuniv.ac.in*

keys which are generated based on the two channels between that relay and the two legitimate nodes respectively. The two legitimate nodes to generate a secret key by combining the broadcast keys with their known keys. We proposed a novel scheme for generating a secret key with the help from multiple colluding relays.

2. BACKGROUND OR RELATED WORK

Earlier the communication in physical layer is to be with trusted relay. We cannot always send the data to the desired IP address through trusted relay because sometimes it may be busy or engaged.Due to the delay, the efficiency of data will be of cost and delay in time may exceed the threshold value.Earlier in trusted relay the name itself defines that the relay is trusted, and no other security issues have to be concerned.The proposed work will focus on the untrusted relay, but while following untrusted relay, some safety measures have to be provided to avoid data loss.

Secrecy is essential for a variety of emerging wireless applications where distributed confidential information is communicated in a multilevel network from sources to destinations. Network secrecy can be accomplished by exploiting the intrinsic properties of multilevel wireless networks (MWNs).[14] Introduces the concept of distributed system secrecy (DNS) and develops a framework for the design and analysis of secure, reliable, and efficient MWNs. The structure accounts for node spatial distribution, multilevel cluster formation, propagation medium, communication protocol, and energy consumption. The paper provides a foundation for DNS and offers a new perspective on the relationship between DNS and network lifetime.

Achieving secrecy in cognitive wireless networks is challenging due to the broadcast nature of the propagation medium. Article [14] introduces the concept of cognitive network secrecy for coexisting primary and secondary networks sharing the same radio resources. A framework for the design and analysis of cognitive networks with secrecy that accounts for their intrinsic properties such as node spatial distribution, wireless propagation medium, and aggregate network interference is presented. the paper envisions that mutual interference between primary and secondary can be beneficial for cognitive system secrecy. It reveals the innate connection between cognitive network secrecy and intrinsic properties of the networks, opening the way to a new paradigm of cognitive system secrecy with interference engineering. The essential premise of physical layer to which have been discussed in [13]. The survey begins with an overview of the foundations dating back to the pioneering work of Shannon and Wyner on information-theoretic security. The paper also describes the evolution of secure transmission strategies from point-to-point channels to multiple antenna systems, followed by generalizations to multiuser broadcast, multiple-access, interference, and relay networks. Secret-key generation and establishment protocols based on physical layer. mechanisms are subsequently covered.

Approaches for secrecy based on channel coding design are then examined, along with a description of interdisciplinary approaches based on game theory and stochastic geometry. The associated problem of physical layer message authentication is also briefly introduced. The survey concludes with observations on potential research directions in this area. 9 coding strategies, or by exploiting the wireless communication medium to develop secret keys over public channels. The survey begins with an overview of the foundations dating back to the pioneering work of Shannon and Wyner on information-theoretic security. We then describe the evolution of secure transmission strategies from point-to-point channels to multiple-antenna systems, followed by generalizations to multiuser broadcast, multiple-access, interference, and relay networks. Secret-key generation and establishment protocols based on physical layer mechanisms are subsequently covered.

The problem of secure transmission in two-hop amplify-and-forward untrusted relay networks is discussed in the article [5] to analyze the ergodic secrecy capacity (ESC) and present compact expressions for the ESC in the high signal-to-noise ratio regime. We also examine the impact of large scale antenna arrays at either the

source or the destination. For large antenna arrays at the source, we confirm that the ESC is solely determined by the channel between the relay and the destination.For large antenna arrays at the destination, we confirm that the ESC is solely determined by the channel between the source and the relay.

3. PROPOSED METHODOLOGY

The user has to do the registration process and get a username and password by which he can get an activated account. For password protection and key matching, the salt algorithm is used in which a random string of data is used to modify a password hash and can be added to the hash to prevent a collision. This is done by uniquely identifying a user's password, even if another user in the system has selected the same password [6]. Password hashmatching strategies are used by the salt algorithm to make it more difficult for an attacker to break into a system because adding salt to a password hash prevents an attacker from testing known dictionary words across the entire system [7]. The salt value should be provided by the intruder, which would require a significant amount of time and space. The length and complexity of the salt value directly affect the time taken for a rainbow table attack [8]. The greater time is required for the success of an attacker by the intruder if the salt is longer and more complicated. For every new hash value we must use new salt and for an intruder, a new dictionary has to be generated for each stored password. In general salt is a random block of data or string or bytes. Figure 1 describes about the process carried out for the proposed methodology.Computer languages provide a different random number of generation classes or functions that are used to generate random numbers and bytes, but these classes and functions are not able to generate cryptographically secure random numbers. These are pseudo-random number generator (PRNG) algorithms which are used by classes and functions in any language because the random value is entirely dependent on data used to initiate the algorithm. So the cryptographically secure pseudo-random number generator (CSPRNG) algorithm is to be required which must produce statically random number, and they must hold up against attack. In some highly secure application special hardware is used to generate the random real number from a physical process such as noise produced by a microphone or nuclear decay of a radioactive source [9]. After generating the true random number called as salt value, it must be combined with the plaintext to produce the salted hash.

To create the salted hash, use salt value as a prefix to the plane text or appending to the plane text before calculating the hash. Steps to generate salt hash password:

1. Get password
2. Generate Salt using trusted random functions/method
3. Append salt to original password
4. Generate Salt Hash password using appropriate hash function
5. Store salt and salt hash in the database.

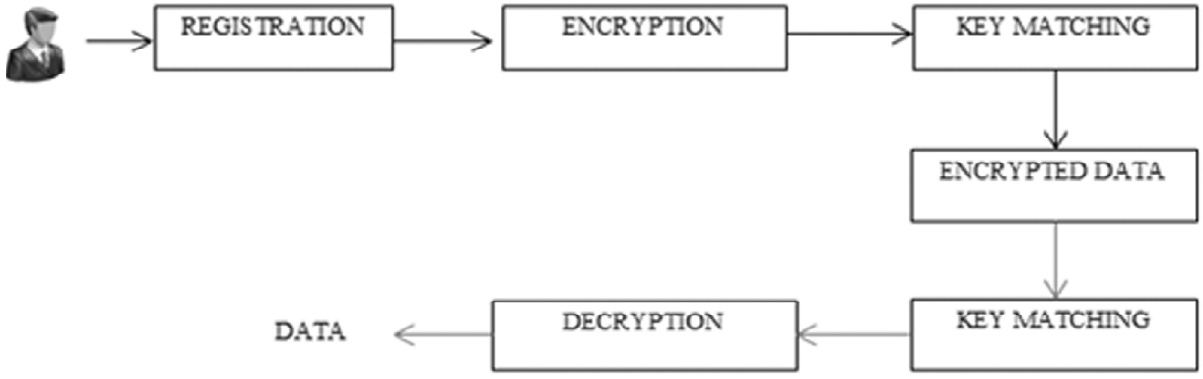

Figure 1: System architecture of the proposed methodology

Using salt password in 17 cryptographically secure random numbers. These are pseudo-random number generator (PRNG) algorithms which are used by classes and functions in any language because the random value is entirely dependent on data used to initiate the algorithm. So the cryptographically secure pseudo-random number generator (CSPRNG) algorithm is to be required which must produce statically random number, and they must hold up against attack. In some highly secure application, hardware is used to generate the random real number from a physical process such as noise produced by a microphone or nuclear decay of a radioactive source [9]. After the random number called as salt value, it must be combined with the plaintext to produce the salted hash. To create the salted hash, use salt value as a prefix to the plane text or appending to the plane text before calculating the the web application, we can prevent SQL Injection attack because many users use the same password for multiple sites to login into an account. The data has to be encrypted and hence RC 4 algorithm is used to provide an enhanced security at frame level especially regarding the added data consumption, by managing both encryption and integrity control into a unique processing. RC4 is a stream cipher, symmetric key encryption algorithm. The same algorithm is used for both encryption and decryption. The data stream is simply XORed with the series of generated keys. The key stream does not depend on the plaintext used. RC4 use 256-bit key length; it performs total 256 rounds of processing to encrypt data. Vernam stream cipher is the most widely used stream cipher based on a variable keysize. It is popular due to its simplicity. It is often used in file encryption products and secure communications, such as within SSL. The WEP (Wireless Equivalent Privacy) protocol also used the RC4 algorithm for confidentiality. It was also used by many other email encryption products. The cipher can be expected to run very quickly in software. It was considered secure until it was vulnerable to the BEAST attack. [12]Privacy is compromised only to the extent that some minimal amount of information is revealed. The complete information that may be revealed is the fact that the e plaintext of a frame is equal to the plaintext of a prior frame. Also, it is revealed only when the plaintext and the header content are equal over two frames. The data get passed through a untrusted relay to reduce the waiting process for trusted relay. The pilot signal gets passed between sender receivers before the data transmission.

Advantages

1. RC4 and SALT algorithms are used to overcome the data efficiency, data loss and time delay.
2. Time taken for transmitting data gets reduced.
3. Data transmission will occur only if the receiver end ready to receive the data.
4. Data will be secured because it gets encrypted using RC4 Algorithm while passing from sender to receiver.
5. Data will get transferred only if the receiver end is ready to receive data.
6. Data-holding between relay will be avoided.

4. EXPERIMENTAL RESULT

The project work towards forwarding the data through a untrusted relay to overcome the delay that occurs while forwarding the data through trusted relay is comparatively more efficient. The time delay in forwarding the data through trusted relay is fixed by transmitting the data through a untrusted relay. The security issue that occurs in transmitting the data through untrusted relay is resolved by encrypting the data using AES algorithm. The results provided by the transmission through untrusted relay are more efficient in terms of time consumption and security of the data.

5. CONCLUSION

We proposed a novel scheme for generating a secret key between two legitimate nodes with the help of multiple untrusted relays, equipped with multiple antennas. The proposed key generation scheme was

designed to achieve highest secret key rate (SKR) for non-partially, and fully colluding modes of relays to adapt to different values of channel coherence time. Through the simulation results, we verified that a secret key can be generated with untrusted relays even for fully and partially colluding cases, and the proposed scheme achieves higher SKR than the prior work. By presenting the existence of the optimal number of untrusted relays, we also verified that exploiting more antennas of untrusted relays cannot always be helpful in achieving a higher SKR. The outcome of our work provide insights on the efficient secret key generation with untrusted relays for various scenarios and open several issues for future research including the effect of interference on SKR and the group key generation with untrusted relays.

6. CONFLICT OF INTEREST

None declared.

REFERENCES

[1] Andrei Sabelfeld and Andrew C. Myers 2003 : A Model for Determining Information Release By –, Software Security: theories and system 2nd Mext_NSF-JSPS international symposium, ISSS.

[2] Ahlswede. R and Csiszar. I Jul. 1993 “Common randomness in information theory and cryptography-Part I: Secret sharing,” IEEE Trans. Inform. Theory, vol. 39, no. 4, pp. 1121–1132.

[3] Bao.V.N. et al. 2013 “Relay selection schemes for dual-hop networks under security constraints with multiple eavesdroppers,” IEEE Trans. Wireless Commun., vol. 12, no. 12, pp. 6076– 6085.

[4] Behrouz A. Forouzan and Debdeep Mukhopadhyay A textbook on Cryptography and Network Security.

[5] Chae. S.H et al. Oct. 2014. “Enhanced secrecy in stochastic wireless networks: Artificial noise with secrecy protected zone,” IEEE Trans. Info. Forensics and Sec., vol. 9, no. 10, pp. 1617– 1628.

[6] Crack Station June, 2013 http://crackstation.net/hashing-security.htm, Retrieved.

[7] He.X and A. Yener Aug. 2010 “Cooperation with an untrusted relay: A secrecy perspective,” IEEE Trans. Inform. Theory, vol. 56, no. 8, pp. 3807–3827.

[8] Liu.Y et al., Oct. 2012 “Exploiting channel diversity in secret key generation from multipath fading randomness,” IEEE Trans. Inform. Forensics and Sec., vol. 7, no. 5, pp. 1484–1497.

[9] http://msdn.microsoft.com/en-us/ library/system.security.cryptography.aspx, Retrived 12th Sep, 2011

[10] Ren.K et al. Aug. 2011"Secret key generation exploiting channel characteristics in wireless communications,” IEEE Wireless Commun., vol. 18, no. 4, pp. 6–12.

[11] Stackoverflow Sep, 2011 , http://stackoverflow.com/questions/244903/why-is-a-password-salt-called-a-salt.

[12] Thai.C.D.T. et al. Dec. 2015"Secret group key generation in physical layer for mesh topology,” in Proc. IEEE Global Commun. Conf. (GLOBECOM).

[13] Wang.L et al. Dec 2014"Secure transmission with optimal power allocation in untrusted relay networks,” IEEE Wireless Commun. Lett., vol. 3, no. 3, pp. 289–292.

[14] Win M.Z et al. 2014. Cognitive network secrecy with interference engineering IEEE Netw., vol. 28, no. 5, pp. 86–90.Ye.C et al. Jun. 2010"Information-theoretically secret key generation for fading wireless channels,” IEEE Trans. Inform. Forensics and Sec., vol. 5, no. 2, pp. 240–254.

[15] Zhang. R et al. Oct 2012 “Physical layer security for two-way untrusted relaying with friendly jammers,” IEEE Trans. Veh.Techn., vol. 61, no. 8, pp. 3693–3704.

[16] Zhou. H et al., Mar. 2014 “Secret key generation in the two-way relay channel with active attackers,” IEEE Trans. Inform. Forensics and Sec.,, vol. 9, no. 3, pp. 476–488

[17] Lai. L et al. “Cooperative key generation in wireless networks,” IEEE Journal on Sel. Areas inCommun., vol. 30, no. 8, pp.1578–1588, Sep. 2012.