International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056
Volume: 04 Issue: 05 | May -2017 www.irjet.net p-ISSN: 2395-0072

A SURVEY ON GROUP KEY AGREEMENT OVER STATE-DEPENDENT WIRELESS BROADCAST CHANNELS

Jaitee Bankar[1], Prof. Jyoti Raghatwan[2]

1 Jaitee Bankar, RMD Sinhgad School of Engineering, Pune, India
2 Prof. Jyoti Raghatwan , RMD Sinhgad School of Engineering, Pune, India

---

Abstract- *Wireless communication is one of the most ubiquitous of modern technologies. There has been considerable recent interest in developing methods for secure data transmission that are based on the physical properties of the radio channel. We focus on secret key generation problem among a group or pair of trusted and authenticated nodes where these nodes communicate over wireless channel in the presence of a passive eavesdropper. There exists a state-dependent wireless broadcast channel from one of the trusted nodes to all other nodes including the eavesdropper. All the trusted nodes can discuss over cost-free noiseless public channel in order to build a common secret key. This discussion can be overheard by the eavesdropper. In the proposed method, a group secret key agreement protocol has been constructed for securely sharing a secret key among group of trusted and authenticated nodes. This is done by converting the broadcast channel into multiple independent erasure channels by using wiretap code. Finally, the best power allocation is obtained by finding the best achievable secret key generation rate.*

Key Words: **Group key agreement, state-dependent wireless broadcast channel, erasure channels, wiretap code, best power allocation**

1. INTRODUCTION

A key agreement is a method where two or more parties agree on a key such that both influence the result. This method allows two or more parties to share a secret key in a secure way. If this is properly done then it precludes undesired third parties form a forcing key selection on the agreeing parties. Several key exchange systems have one party generate the key and merely send that key to other party. The other party has no influence on that key. By using a key agreement protocol some of the key distribution problems can be avoided which are associated with such type of systems. Protocols in which both the parties manipulate the final derived key is the single way to implement perfect forward secrecy.

Wireless communication channels are easier to eavesdrop and harder to secure – even towards unintentional eavesdroppers. As an example, consider a sender, Alice, who wants to send private messages to multiple receivers, Bob, Claire and Donald, within her transmission radius, and assume public feedback from the receivers to Alice. When Alice broadcasts a message intended for Bob, Claire and Donald try to overhear, as the side information they possibly collect can enable Alice to make her following broadcast transmissions more efficient. But then, this collected side information would allow Claire and Donald to learn parts of Bob's message. Claire and Donald could try to put together the parts they overheard, to extract increased information about Bob's message. In such a setting, can we keep the message for each user information theoretically secure from the other users, even if these nodes collaborate. Nearly all the protocols assume that the eavesdropper does not have access to broadcast transmissions and there should be perfect knowledge about the eavesdropper's channel. Most of the protocols are less computationally efficient.

Thus, a group secret key generation among group of trusted nodes that communicate over wireless channels in the presence of a passive eavesdropper and that has access to the noisy broadcast transmissions is a complex problem to be solved.

In this paper, we have surveyed on group key agreement over state-dependent wireless channels. Section 2 of this paper deals with Literature Survey and Section 3 presents Proposed System. Section 4 concludes this paper.

2. LITRATURE SURVEY

A comprehensive literature survey was performed in the support of the group key agreement problem. In literature, several techniques have been presented for allowing two or more parties to securely share a secret key. In the network security area, the group key agreement problem is considered to be the one of the most challenging task that tries to address the issue of securely sharing a secret key between two or more parties. The group key agreement over wireless channels is the main difficulty for securely sharing the secret key among multiple parties. A number of methods have been proposed in order to solve the complexity observed in the group key agreement. Group key agreement still remains difficult task.

An information theoretically secure secret key agreement protocol has been developed in [1]. The best achievable secret key generation rate has been found in order to solve a non-convex power allocation problem over the erasure channels. The Secret Key Generation (SKG) capacity problem among multiple terminals over state-dependent Gaussian broadcast channel in the presence of eavesdropper is still unsolved. In [2], the two transmitter

multiple-access channel with noncausal side information (NSI) at one single-sided or both two-sided of the encoders in the presence of an external wire tapper and below collective and individual secrecy constraints have been studied. The main drawback of this scheme is that the secrecy rate increases with the number of encoders.

The problem of how multiple users can agree on a single secret key by public discussion if users have access to a private discrete memory less multi-terminal channel has been studied in [3]. For the special private networks where each user can either transmit or receive but not both, it is not possible to adapt the channel inputs privately to the channel outputs. The secrecy generation for multi-access channel models has been considered in [4], whose resources contain facilities for secure noisy channel broadcast from the input to the output terminals, public noiseless communication amongst all the terminals and mutually independent randomization at the terminals. In this scheme, secrecy rates cannot be achieved by the simple protocols entailed by general source emulation and complex protocols are required.

A protocol that enables a group of terminals, connected to the similar broadcast domain in order to exchange pairwise secrets in the presence of an adversary has been developed in [5]. The protocol secrecy rate increases as the network presence of the adversary increases. A novel approach to analyze the capacity of Gaussian relay networks has been presented in [6]. The cutset bound gap grows with the number of nodes in the network is the main limitation of this approach.

In [7], the problem of information theoretically secure secret key agreement under the well known source model and channel model has been studied. The proposed method for solving this problem has the limitation of not achieving the optimal secret key generation rate.

3. PROPOSED SYSTEM

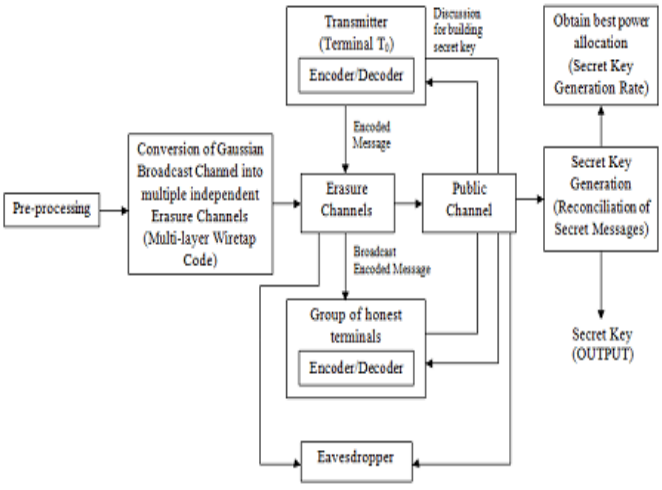

Figure 1: Proposed System Architecture

There is no universal methodology that can be used for group key agreement. Key generation protocols have a long history of new protocols improving over past work in various aspects such as efficiency, features or security. However, this history is also paved with numerous flaws in many protocols which got only discovered later. Most of these flaws are due to an ad-hoc security analysis and due to overlooking various attacks. Building the protocol with systematic design and following prudent design and engineering principles can greatly reduce this risk. However, only a sound underlying formal model and rigorous security proofs can give real assurance of security. The majority of works employed in this domain fall under constructing secure protocols for group key agreement.

The proposed system follows the general five-step framework: preprocessing; conversion of state-dependent Gaussian broadcast channels into multiple erasure channels; broadcasting message regarding common secret key generation; discussion over public channel to build secret key and obtaining best power allocation as shown in figure 3. The first step is to notify each terminal of the key agreement event starting from Terminal T_0 and there exists Gaussian broadcast channel from Terminal T_0 all the other honest nodes of the group. This is the starting assumption and it should be satisfied. All the honest nodes generate random variable at time index t = 0.

The second step is conversion of Gaussian broadcast channel into multiple independent erasure channels by using multi-layer wiretap code. The third step is broadcasting message regarding secret key generation over the multiple independent erasure channels. Fourth step consists of discussion of honest terminals over public channel in order to build secret key and reconciliation of secret messages of the honest terminals to generate a common secret key and the last step is to obtain best power allocation by finding the best achievable secret key generation rate.

4. CONCLUSION

In this paper, we surveyed the group key agreement techniques and studied the group key agreement problem for solving the secret key generation problem among a group of trusted and authenticated nodes that perform communication over wireless channels in the presence of a passive eavesdropper. A group secret key agreement protocol has been presented that solves the secret key generation problem over wireless channels. A group key agreement in this setting is very suitable for applications such as social networks.

ACKNOWLEDGEMENT

It is my privilege to acknowledge with deep sense of gratitude to my guide Prof. Jyoti Raghatwan for her kind cooperation, valuable suggestions and capable guidance and timely help given to me in completion of my paper. I express my gratitude to Prof. Vina M. Lomte, Head of Department,

RMDSSOE (Computer Dept.) for her constant encouragement, suggestions, help and cooperation.

REFERENCES

[1] M. Siavoshani, S. Mishra, S. Diggavi, and C. Fragouli, "Multi-Party Secret Key Agreement Over State-Dependent Wireless Broadcast Channels," IEEE Transactions on Information Forensics and Security, Vol. 12, No. 2, 2017.

[2] A. Sonee and G. A. Hodtani, "On the secrecy rate region of multiple access wiretap channel with non causal side information," IEEE Trans. Inf. Forensics Security, vol. 10, no. 6, pp. 1151-1166, 2015.

[3] C. Chan and L. Zheng, "Multi-terminal secret key agreement," IEEE Trans. Inf. Theory, vol. 60, no. 6, pp. 3379-3412, Jun. 2014.

[4] I. Csiszar and P. Narayan, "Secrecy generation for multi access channel models," IEEE Trans. Inf. Theory, vol. 59, no. 1, pp. 17-31, Jan. 2013.

[5] I. Safaka, C. Fragouli, K. Argyraki, and S. Diggavi, "Exchanging pairwise secrets efficiently," in Proc. IEEE INFOCOM, Apr. 2013.

[6] A. S. Avestimehr, S. N. Diggavi, and D. N. C. Tse, "Wireless network information flow: A deterministic approach," IEEE Trans. Inf. Theory, vol. 57, no. 4, pp. 1872-1905, Apr. 2011.

[7] A. A. Gohari and V. Anantharam, "Information-theoretic key agreement of multiple terminals - Part I," IEEE Trans. Inf. Theory, vol. 56, no. 8, pp. 3973-3996, Aug. 2010.