Group Key Establishment Scheme Using Wireless Channel Status

Seon Yeob Baek and Jongwook Park
The Attached Institute of Electronics and Telecommunications Research Institute (ETRI),
P.O.Box #1, Yuseong-gu, Daejeon, 305-600, Korea
E-mail: sybaek@ensec.re.kr and khspjw@hotmail.com

***Abstract*—Broadcast-based wireless communication is vulnerable to sniffing and eavesdropping by adversaries. Hence, wireless network security mechanisms have relied on cryptographic algorithms to protect information and support confidentiality. We propose a group key establishment scheme for secure wireless multicast services without a key management center. The proposed scheme exploits wireless channel reciprocity and generates an identical secret key among group users by steering pilot phase. We analyze and evaluate performance of the proposed scheme. Our results give an insight to determine transmit power strength and phase quantization-level according to the number of group users and group key size.**

***Index Terms*—Group key generation;group key establishment;secret key generation;secret key establishment;physical layer security**

I. Introduction

Security is a critical issue in wireless communication applications. Naturally, the wireless communication is based on broadcast of signal. Hence, if the signal is not encrypted, malicious adversaries can eavesdrop on the wireless communication and acquire the secret information from wireless sniffing. Most wireless network security mechanisms have relied on cryptographic algorithms to protect information and support confidentiality. The cryptographic algorithms require secret key establishment between users in a secure fashion. Key establishment consists of key generation and agreement. Secret keys are typically generated by the random number generator. Famous key agreement solution is Diffie-Hellman (D-H) algorithm [1]. The D-H algorithm is aimed at deriving symmetric keys over a unsecure channels. However, the D-H algorithm requires fast exponentiation and this is a cumbersome operation for mobile devices. Meanwhile, a key management center has been proposed to generate secret key and distribute the secret key securely. However, availability of the key management center is no longer guaranteed in adhoc networks. Therefore, key establishment has become more challenging in infrastructureless wireless networks [2].

There is increasing interest in utilizing wireless characteristics to improve wireless security [3]. The underlying wireless channel response between two users is unique, decorrelated rapidly in space, and dynamic in time. Hence, the wireless communication systems can utilize these characteristics to meet security requirements. The unique and decorrelated wireless characteristics can substitute traditional authentication protocols as a physical layer fingerprint [4]–[7]. Moreover, the dynamic and decorrelated wireless characteristics can provide randomness and uniqueness of secret key. Since eavesdroppers cannot infer the wireless channel response between two users, the wireless channel response becomes a basis to create common secret key in wireless networks [8]–[11]. Wireless channel reciprocity also supports simplified and secure secret key agreement scheme with time division duplex (TDD) mode. Since the wireless channel response of pilot signal has been already utilized for equalization or adaptive modulation and coding (AMC) scheme, wireless channel characteristic-based security schemes does not request additional radio resources for applications.

A variety of secret key establishment schemes based on radio channel reciprocity have been proposed to exploit various channel characteristics. Kai and Yunchuan have proposed the received signal strength (RSS)-based key establishment scheme using multiple antennas and adaptive channel probing, respectively [8], [9]. Suhas *et al* have proposed the level crossing-based key establishment scheme [10]. The RSS-based schemes have difficulty on quantization-level decision to acquire uniformly random sequence. On the other hand, the level crossing-based scheme needs guard area to reduce signal variation sensitivity. Qian *et al* have proposed a random phase-based pairwise and group key establishment scheme [11]. The phase-based key establishment scheme can achieve uniformly random key sequence and is controllable by a transmitter.

Previous wireless channel characteristic-based key establishment schemes have focused on peer-to-peer secret key. However, multiple users should share the common secret key for secure wireless multicast services. Qian *et al* have studied the wireless channel characteristic-based group key establishment scheme utilizing phase of the received signal [11]. Group users rotate pilot transmission and reception in multiple frames. Since duration time for key establishment is proportional to the number of users, the channel reciprocity might not be guaranteed in multiple frames for a large number of users. Key agreement probability (KAP) also decreases due to propagation of phase estimation error. Hence, we propose a novel group key establishment scheme for the secure wireless multicast services. The proposed scheme exploits wireless channel reciprocity and generates group key adjusting pilot phase only in a frame. To start group key establishment, group users select one master who can control pilot signal among them and others becomes clients. The master determines

TABLE I
NOTATIONS

Parameter	Definition
h_i	Channel gain of user i
M	Group key size
L	Number of group users
q	Quantization level
T	Frame duration
P_{sa}^{G}	Successful group SAP
θ	Phase of channel response
$\tilde{\theta}$	Estimated phase
κ	Group key
$h(\kappa)$	Hash value of group key

phase offset of clients and transmits phase-steered pilot signal according to each client's channel response. From the received pilot signal, clients can generate an identical group key.

The rest of this paper is organized as follows. In Section II, we propose a novel group key generation and agreement scheme based on phase steering. We analyze the proposed group key establishment scheme in Section III and evaluate performance of the proposed scheme according to the number of users and quantization level in Section IV. Finally, we present conclusion and future work in Section V.

II. GROUP KEY ESTABLISHMENT SCHEME

Multicast transmission is an efficient method when multiple users request identical information. In order to improve information security, multicast data should be encrypted by shared secret key among group users. However, it has been a tough issue to generate a group key and distribute the group key securely without a key management center. We propose a novel group key establishment scheme using wireless channel status.

Table I lists notations used in this paper and Fig. 1 shows wireless network environments for multicast transmission. There are six group users and two eavesdroppers. The eavesdroppers try to sniff data over the wireless channel. To start a novel group key establishment, group users select one master to generate group key among them and other users become clients. Wireless links, h_i, between master and each client i are independent of one another. The master transmits group key information hiding through wireless channel response. It is assumed the eavesdroppers have uncorrelated wireless channel with users. Hence, the eavesdroppers have no way of estimating channel response between the master and clients. The proposed key establishment scheme is scalable by relaying identical group key to other clients.

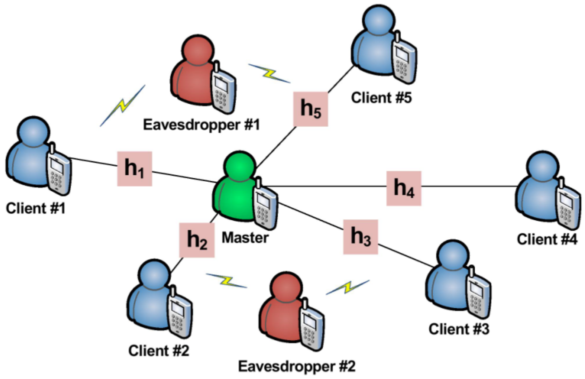

Fig. 1. Network Environment

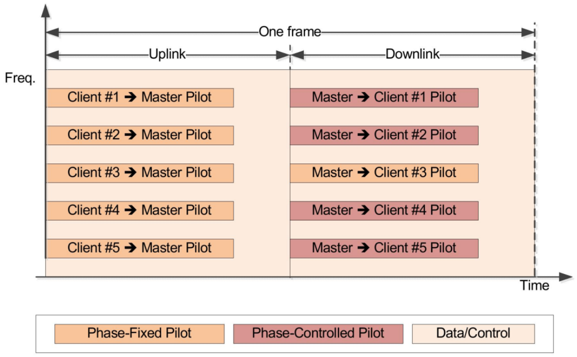

Fig. 2. Frame Structure

Fig. 2 shows one example of frame structure for the proposed group key establishment scheme. The selected master utilizes pilot resource of each client for fast key generation. The wireless communication system supports TDD mode. One frame consists of uplink and downlink modes. In uplink mode, clients transmit phase-fixed identical pilot signal to the mater. In downlink mode, the master transmits phase-controlled pilot signal to clients according to channel response of each client. Since the pilot signal is controlled only during key generation period, phase-controlled pilot does not affect equalization or AMC scheme. Other resource except pilot signal is utilized to transmit data or control signal. It is assumed wireless channel response is quasi-static during key generation and thus users can exploit channel reciprocity.

Group key size and the number of users in a group is denoted as M bits and L, respectively. There are q symbols or quantization level. Hence, generated bits from one symbol is $\log_2 q$ bits. Successful symbol agreement probability (SAP) among group users and frame duration is denoted as P_{sa}^{G} and T, respectively. Then, expected group key generation time, $E[T_k]$, is proportional to

$$E[T_k] \propto \frac{M \cdot T}{\log_2 q \cdot P_{sa}^{G}}. \quad (1)$$

Fig. 3 describes the procedure of a proposed group key establishment scheme. The group key establishment scheme is divided into two steps as follows: group key generation and group key agreement between a master and clients.

In the first step, a client transmits a phase-fixed pilot signal, s_{12}, to a master. Then, the master estimates phase of the wireless channel response of the client, $\tilde{\theta}_{12}$. Meanwhile, there are candidate q pilot symbols to be transmitted by the master. These symbols are equally distanced for uniform randomness of the group key and each symbol represents unique binary sequence. The master selects one of candidate pilot symbols randomly and evaluate phase of the selected symbol, θ. The selected pilot symbol is applied identically to every client.

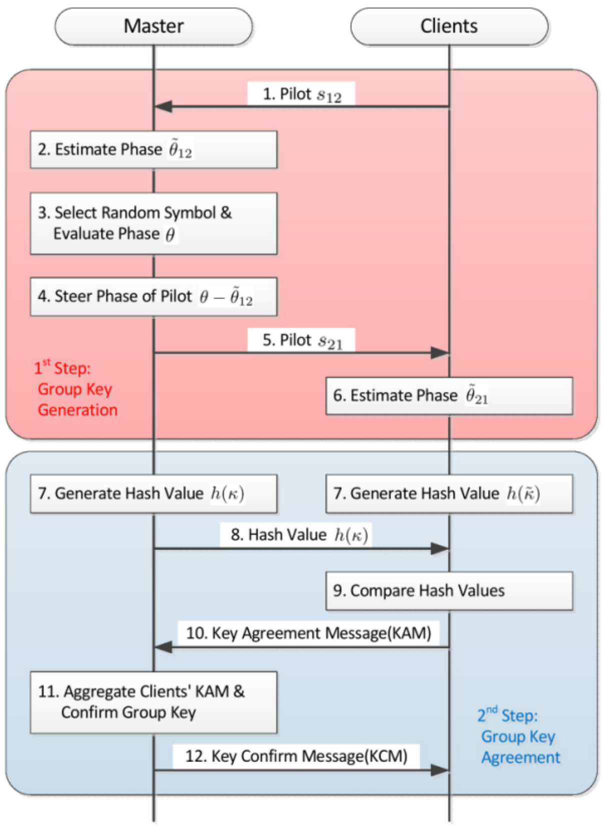
Master
Clients
1. Pilot s_{12}
2. Estimate Phase $\tilde{\theta}_{12}$
3. Select Random Symbol & Evaluate Phase θ
4. Steer Phase of Pilot $\theta - \tilde{\theta}_{12}$
5. Pilot s_{21}
1st Step: Group Key Generation
6. Estimate Phase $\tilde{\theta}_{21}$
7. Generate Hash Value $h(\kappa)$
7. Generate Hash Value $h(\tilde{\kappa})$
8. Hash Value $h(\kappa)$
9. Compare Hash Values
10. Key Agreement Message(KAM)
11. Aggregate Clients' KAM & Confirm Group Key
2nd Step: Group Key Agreement
12. Key Confirm Message(KCM)

Fig. 3. Group Key Generation Procedure

From the selected symbol, the master compute phase offset, $\theta - \tilde{\theta}_{12}$. The master steers pilot phase according to the phase offset and transmits phase-steered pilot signal to the client. After pilot reception, the client estimates phase of the channel response, $\tilde{\theta}_{21}$ and extracts secret bits from $\tilde{\theta}_{21}$. The master and the client generate group key sequence aggregating secret bits from randomly selected symbol and estimated phase of the channel response, respectively. If the aggregated secret bit sizes are equal to the group key size, the master and the client finishes key generation and derives group key, κ and $\tilde{\kappa}$, respectively. Error correction code can be utilized for group key reconciliation.

In the second step, the master and the client generates hash value of the generated group key, κ and $\tilde{\kappa}$, respectively. Then, the master transmits hash value, $h(\kappa)$, to the client and the client compares the hash value with its own hash value, $h(\tilde{\kappa})$. Transmission of hash value can reduce data size to transmit and prevent sniffing. From comparison result, the client transmits key agreement message (KAM) that includes group key agreement information. The master aggregates KAMs received from multiple clients and confirms group key from KAMs. If every client has identical hash value with the master's hash value, the master transmits key confirm message (KCM) to clients. Otherwise, the master transmits key regeneration message (KRM) to clients and they restarts group key generation step.

To simply this procedure, an alternative scheme without KAM transmission is also possible. Every client transmits $h(\tilde{\kappa})$ to the master before the master transmits KAM. In this case, the master compares hash values received from clients and transmits KCM or KRM to clients. We can select one of two schemes adequately with regard to data size to be transmitted for key agreement.

III. Analysis of Group Key Establishment Scheme

We consider channel gain and noise at receiver for analysis model. Wireless channel gain has Rayleigh distribution and additive noise is zero-mean complex Gaussian random variables. From channel reciprocity, group users share the quasi-static wireless link. A master and a client experiences an identical channel gain but independent additive noise, respectively.

Pilot signal from the client to the master at time t is expressed as

$$s_{12}(t) = \exp[j(w_c(t - t_d))], \tag{2}$$

where w_c and t_d denotes carrier frequency and one-way link delay time, respectively.

Received signal at the master is expressed as

$$r_{12}(t) = h \cdot \exp[j(w_c t + \theta_{12})] + n_{12}, \tag{3}$$

where h, θ_{12}, and n_{12} denotes channel gain, shifted phase from channel response, and additive noise at the master, respectively. From the received signal (3), the master estimates phase of the channel response as $\tilde{\theta}_{12} = \theta_{12} + \theta_{12}^n$ due to the additive noise.

After pilot reception, the master selects one of candidate symbols randomly and evaluates phase, θ, from the selected symbol. Similar to M-ary Phase Shifting Keying (PSK), phases of candidate symbols are equally distanced and each phase denotes specific bit sequences such as Gray code. In order to derive an identical symbol, the master transmits controlled pilot signal according to the estimated phase offset, $\tilde{\theta}_{12}$, delay time, t_d, and normalized estimated channel gain, $|r_{12}|$. Hence, the pilot signal from the master to the client is expressed as

$$s_{21}(t) = \frac{\exp[j(w_c(t - t_d) + \theta - \tilde{\theta}_{12})]}{|r_{12}|}. \tag{4}$$

After the client receives pilot signal from the master, she or he recovers transmitted symbol and extracts secret key bits. The received signal at the client is expressed as

$$r_{21}(t) = \frac{h}{|r_{12}|} \cdot \exp[j(w_c t + \theta + \theta_{21} - \tilde{\theta}_{12})] + n_{21}. \tag{5}$$

The estimated phase at the client is denoted as $\tilde{\theta}_{21}$ and is equal to $\theta + \theta_{21} - \tilde{\theta}_{12} + \theta_{21}^n$. Since θ_{12} is identical to θ_{21}, $\tilde{\theta}_{21}$ is derived as $\theta + \theta_{21}^n - \theta_{12}^n$. The estimated phase error at the clients becomes $\theta_{21}^n - \theta_{12}^n$ and shows similar distribution with M-ary PSK transmission in Rayleigh channel [12]. Joint probability density function (PDF) of received signal vector r, and angle θ, is obtained as

$$p(r,\theta) = \frac{r}{\pi N_0} \exp\left\{\frac{1}{N_0}(r^2 - 2\alpha\sqrt{2E_s}r\cos\theta + 2\alpha^2 E_s^2)\right\}, \tag{6}$$

where N_0 is noise variance, α is channel gain of the received signal, and E_s is symbol energy. Since we are interested only in the angle, we obtain the marginal pdf of angle as

$$\begin{aligned} p(\theta) &= \int_0^\infty p(r,\theta)dr \qquad (7) \\ &= \frac{1}{\pi}\exp(-2\gamma\sin^2\theta) \\ &\quad \times \int_0^\infty x\exp\left(x-\sqrt{2\gamma}\cos\theta\right)^2 dx, \qquad (8) \end{aligned}$$

where γ is the received symbol energy-to-noise ratio.

For q symbol-level quantization, symbol error probability (SEP) with Es/No value of γ is expressed as

$$\begin{aligned} P_q(\gamma) &= 1-\int_{-\pi/q}^{\pi/q} p(\theta)d\theta \qquad (9) \\ &\approx \sqrt{\frac{2}{\pi}}\int_{\sqrt{2\gamma}\sin\frac{\pi}{q}}^{\infty} \exp\left(-\frac{x^2}{2}\right)dx \qquad (10) \\ &= 2Q\left(\sqrt{2\gamma}\cdot\sin\frac{\pi}{q}\right), \qquad (11) \end{aligned}$$

where $Q(x)=\frac{1}{\sqrt{2\pi}}\int_x^\infty e^{-\frac{u^2}{2}}du$.

The wireless channel gain follows Rayleigh distribution and is expressed as

$$p_\gamma(x)=\frac{1}{\gamma}\exp\left(-\frac{x}{\gamma}\right). \qquad (12)$$

From (11) and (12), symbol agreement probability (SAP) of user i is expressed as

$$P^i_{sa}=\int_0^\infty P_q(x)p_\gamma(x)dx. \qquad (13)$$

Finally, probability of successful SAP among L group users, P^G_{sa}, is derived as

$$P^G_{sa}=\prod_{i=1}^{L-1}P^i_{sa}. \qquad (14)$$

IV. Performance Evaluation

We evaluate and compare the performance of the proposed group key establishment scheme with computer simulation results in this section.

Fig. 4 shows the SEP of the proposed scheme in Rayleigh channel. Solid lines and symbols represent the analytic and simulation results, respectively. The analytical results are quite analogous to the simulation results. Rayleigh channel gain, additive noise and quantization level affect the performance of SEP. As quantization level decreases or the value of Es/No increases, the performance of SEP is improved because Hamming weight between each symbol increases. To meet 1[%] of SEP, each quantization level of 2, 4, 8, 16 requires 15, 20, 25, 30[dB] of Es/No, respectively. This means approximately additional 5[dB] transmit signal strength enhancement is required to generate group key two times faster in Rayleigh channel environments. Fig. 5 shows the SEP of the proposed scheme without channel gain normalization. In this case, $|r_{12}(t)|$ in (4) is fixed to one. Therefore, the channel gain affects the estimated phase severely and thus shows worse performance compared to the proposed scheme with channel gain normalization.

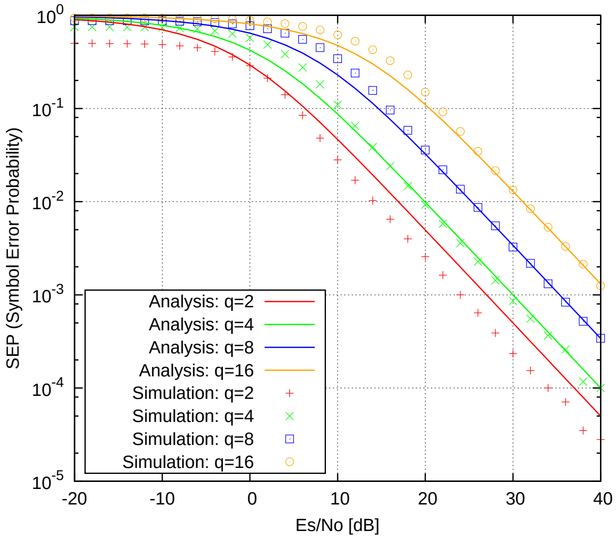

Fig. 4. Symbol error probability(SEP) of the proposed group key establishment scheme in Rayleigh channel

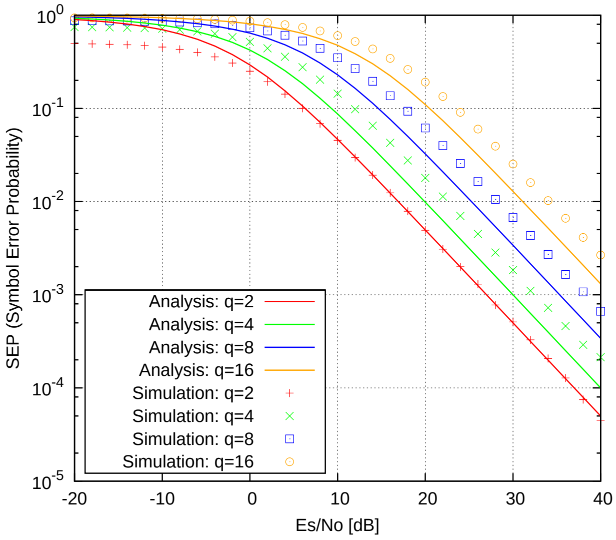

Fig. 5. Symbol error probability(SEP) of the proposed group key establishment scheme without channel response normalization in Rayleigh channel

Fig. 6 shows the SAP of the proposed scheme for varying the number of group users. Each line and symbol represents quantization level and the number of group users except one master, respectively. As quantization level increases, the performance of SAP is worsened because Hamming weight between each symbol decreases. As the number of group users increases, high symbol energy is required to derive an identical key among group users. Every group user might have an identical key symbol approximately above 25[dB] of Es/No regime.

From (1), there is a tradeoff between quantization level, q,

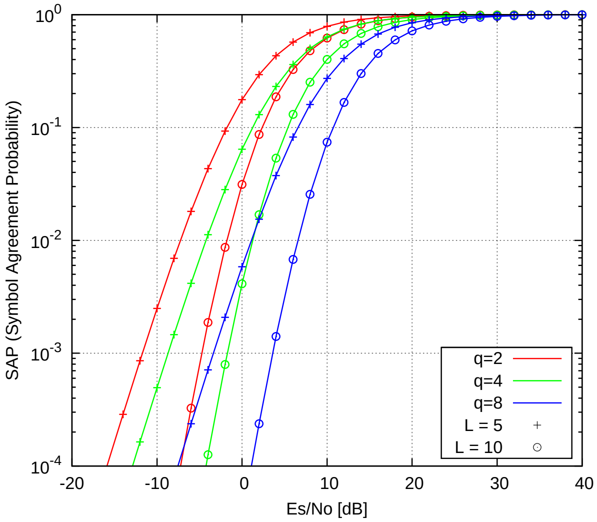

Fig. 6. Symbol agreement probability(SAP) of the proposed group key establishment scheme for varying the number of group users and quantization level in Rayleigh channel

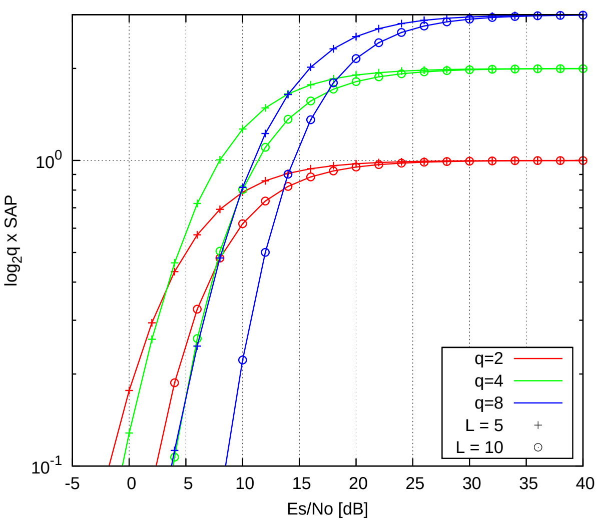

Fig. 7. Key generation rate of the proposed group key establishment scheme for varying the number of group users and quantization level in Rayleigh channel

TABLE II
THRESHOLD VALUES FOR QUANTIZATION LEVEL SELECTION

L	q	Threshold Values [dB]
5	$2 \Leftrightarrow 4$	3.3
5	$4 \Leftrightarrow 8$	13.9
10	$2 \Leftrightarrow 4$	7.7
10	$4 \Leftrightarrow 8$	17.6

and SAP, P_{sa}^G, to reduce group key establishment time. Higher quantization level generates more secret bits per a sample but results in degradation of SAP. Therefore, appropriate quantization level and transmit power strength is required to achieve fast group key establishment.

Fig. 7 shows key generation rate of the proposed group key establishment scheme for varying the number of group users. From Fig. 7, the threshold value of Es/No determine quantization level, q. For five group users, 3.3[dB] and 13.9[dB] of Es/No is the threshold value to transmit quantization level from 2 to 4 and 4 to 8, respectively. For ten group users, 7.7[dB] and 17.6[dB] of Es/No is the threshold value to transmit quantization level from 2 to 4 and 4 to 8, respectively. Table II lists threshold values for quantization level selection for varying the number of group users. As the number of group users increases, the required Es/No values also increases to utilize high order of quantization level.

V. CONCLUSION AND FUTURE WORK

In this paper, we have proposed a phase-based group key establishment scheme using wireless channel status. With phase steering of the master, every group user can generate an identical group key without the key management center. Our analysis model evaluates performance of the proposed group key establishment scheme in terms of SEP and SAP for varying Es/No, the number of group users, and quantization-level. The evaluated performance of the proposed scheme gives an insight to determine transmit power strength and quantization-level according to the number of users and group key size. The proposed scheme can establish group key efficiently for wireless multicast services in infrastructureless networks. Our future work is to implement the proposed scheme and perform field test using SDR Platform.

REFERENCES

[1] W. Diffie and M. Hellman, “New directions in cryptography,” *IEEE Information Theory*, vol. 22, no. 6, pp. 644-654. November 1976.

[2] Y.-S. Shiu, S. Y. Chang, H.-C. Wu, S. C.-H. Huang and H.-H. Chen, “Physical Layer Security in Wireless Networks: A Tutorial,” *IEEE Wireless Communications*, vol. 18, no. 2, pp. 66-74. April 2011.

[3] R. Liu and W. Trappe, *Securing Wireless Communications at the Physical Layer,* Springer, 2009.

[4] J. Pang, B. Greenstein, R. Gummadi, S. Seshan, and D. Wetherall, “802.11 User Fingerprinting,” in *Proc. of ACM MobiCom*, Montréal, Canada, September 2007, pp. 99-110.

[5] V. Brik, S. Banerjee, M. Gruteser, and S. Oh, “Wireless Device Identification with Radiometric Signatures,” in *Proc. of ACM MobiCom*, San Francisco, USA, September 2008, pp. 116-127.

[6] L. Xiao, L. Greenstein, N. Mandayam, and W. Trappe,“Using the Physical Layer for Wireless Authentication in Time-variant Channels,” *IEEE Transactions on Wireless Communications*, vol. 7, no. 7, pp. 2571-2579. July 2008.

[7] K. Zeng, K. Govindan, and P. Mohapatra, “Non-Cryptographic Authentication and Identification in Wireless Networks,” *IEEE Wireless Communications*, vol. 17, no. 5, pp. 56-62. October 2010.

[8] K. Zeng, D. Wu, A. Chan, and P. Mohapatra, “Exploiting Multiple-Antenna Diversity for Shared Secret Key Generation in Wireless Networks,” in *Proc. of IEEE INFOCOM*, San Diego, USA, March 2010, pp. 1-9.

[9] Y. Wei, K. Zeng, and P. Mohapatra, “Adaptive Wireless Channel Probing for Shared Key Generation,” in *Proc. IEEE INFOCOM*, Shanghai, China, April 2011, pp. 2165-2173.

[10] S. Mathur, W. Trappe, N. Mandayam, C. Ye, and A. Reznik, “Radio-telepathy: Extracting a Secret Key from an Unauthenticated Wireless Channel,” in *Proc. of ACM MobiHoc*, San Francisco, USA, September 2008, pp. 128-139.

[11] Q. Wang, H. Su, K. Ren, and K. Kim, “Fast and Scalable Secret Key Generation Exploiting Channel Phase Randomness in Wireless Networks,” in *Proc. of IEEE INFOCOM*, Shanghai, China, April 2011, pp. 1422-1430.

[12] J. Proakis, *Digital Communications,* Mc Graw Hill, 2000.