Implementation of Frequency Quorum System for Securing Physical Layer in Wireless Smart Grid

Halim Halimi
Department of IT
State University of Tetovo
Tetovo, Rep. of Macedonia
hhalimi2000@yahoo.com

Aristotel Tentov
Computer Science and Engineering Department
Faculty of Elec. Engin. and Information Technologies
Skopje, Rep. of Macedonia
toto@feit.ukim.edu.mk

Abstract. **The Smart grid is the next generation power grid, which consists of a power grid and an information and communication technology system. Communication networks play a critical role in smart grid, as the intelligence of smart grid is built based on information exchange across the power grid. In power transmission segments of smart grid, wired communications are usually adopted to ensure robustness of the backbone power network. In contrast, for a power distribution grid, wireless communications provide many benefits such as low cost high speed links, easy setup of connections among different devices/appliances, and so on. Wireless communications are usually more vulnerable to security attacks than wired ones. Developing appropriate wireless communication architecture and its security measures is extremely important for a smart grid system. This work addresses physical layer security in a Wireless Smart Grid. To understand new types of threats, we review fundamentals of wireless communication and examine physical attack models. Hence a defense Quorum-based algorithm is proposed to ensure physical security in wireless communication.**

Keywords**: Physical layer security, wireless smart grid, wireless security.**

I. INTRODUCTION

Generally, the smart grid is a power delivery infrastructure that can increase the efficiency, reliability and flexibility of the electricity networks through two way flows of electricity and information. With the use of advanced sensing technologies and control methods the smart grid may provide predictive information and corresponding recommendation to all stakeholders (utilities, suppliers and consumers). The systems also offers intelligent services such as appliance control for energy efficiency and integration of Distributed Energy Resources (DER) [1]. In this sense the smart grid is a "system of heterogeneous systems" and devices over various domains. This complex presents many challenges in the cyber security and privacy aspect. For securing such a complex systems, different security technologies, such as Public Key Infrastructure (PKI), Intrusion Detection Systems (IDS), Virtual Private Network (VPN), antivirus software, firewalls etc., are used. An enterprise network is built on the Ethernet using the Internet Protocol (IP). The world's largest public network, the Internet, may interconnect them.

Wireless communication offers many benefits over wired technologies, including mobility, access to information, reduced installation and maintenance cost and support for interoperability. Instead of these benefits, there are a number of challenges that remain, such as: network performance, suitability, interoperability and security.

In this work we propose to use Frequency Quorum Rendezvous (FQR) scheme, instead of classical FHSS. FQR offers two benefits: First FQR decreases time latency. Second, FQR does not require any pre-known sequence about frequency hopping, which is faster and robust against attacks. In [2], FQR is used for key establishment under jamming attack. In work [3], FQR was used for cognitive radios to avoid random interference.

In the remainder of this article we first introduce an overview of wireless technologies and architecture in the smart grid, as well as general security threats that will have to be faced with and the corresponding solution. Further follows a deep analysis of proposed FQR scheme to enhance fast and robust communication in wireless network. Moreover, we present a summary of the Physical Layer Security and an overview of attacks and threats on the physical layer of wireless networks in the smart grid. After that we evaluate the proposed algorithm and finally, we conclude this work.

II. WIRELESS TECHNOLOGIES AND ARCHITECTURE IN SMART GRID

A. Wireless Technologies in Smart Grid

The National Institute of Standards and Technologies (NIST) has investigated and proposed a complex infrastructure for smart grid based on a set of seven domains [4]: bulk, generation, energy distribution, power transmission, operation and control, market, service providers and customers. The public key infrastructure (PKI) is considered as a key security technology for various smart grid communication networks. Security problems of networking in smart grid are focused on the Internet, wireless networks, sensor networks, through an Advanced Metering Infrastructure (AMI). An AMI is an interface with the opportunities for managing and interacting with smart devices and others utility systems through a two way communication infrastructure. Also multiple networking technologies can be utilized for the smart grid, including fiber

optics, Land Mobile Radio (LMR), 3G/4G (WiMax), WiFi and so on. Which one will be used depends on the smart grid environment. There are several applications and technologies integrated in an AMI system including: smart meters, Home Area Networks (HAN), Wide Area Communication Infrastructure, Meter Data Management Systems (MDMS) and operational gateways.

B. Wireless Network Architecture in Smart Grid

In the academic research area several architectures for implementing smart grid privacy are proposed. In general, each smart grid network architecture is consisted of three basic layers: at the top layer is a control center maintained by the power operator, the second layer presents the distributed network, consisted of several substations inside, where each is responsible for the power supply of an area and the lowest layer consists of a set of end devices and a smart meter collecting data from the devices. Using IEEE 802.15 standard they form a wireless sensor network and ZigBee smart profile as shown in Figure 1 [5].

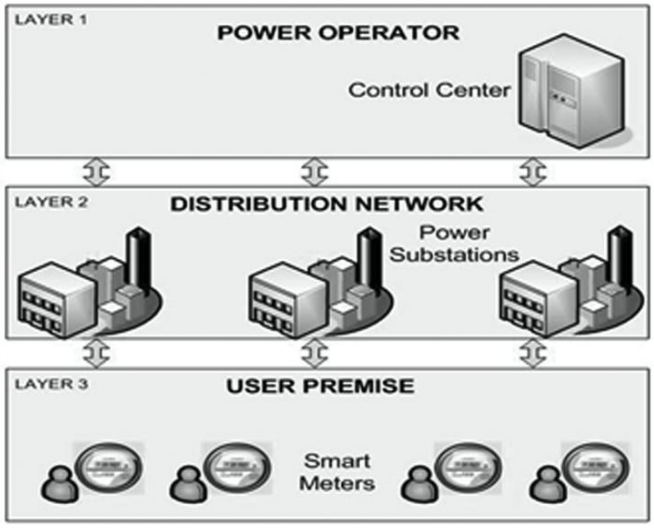

Figure 1. A three layer wireless network architecture in smart grid [5].

C. Wireless Channel

The standard 802.11b uses the 2.4 GHz frequency band. The band is divided into 11 channels. Each channel is a contiguous band of frequencies 22 MHz wide and the center frequencies are 5 MHz apart. Channel 1, for instance, operates from 2,401 GHz to 2,423 GHz (2.412 GHz $\pm$ 11MHz); channel 2 operates from 2.406 to 2.428 GHz (2.417 $\pm$ 11 MHz), and so forth. Transmitting a wireless signal implies that the sender uses the center frequency of a pre-defined channel and the signal does not interfere with any non-overlapping channels within the band. The receiver must be in the same channel with the sender in order to receive the signals correctly.

III. ENABLING FAST AND ROBUST COMMUNICATION USING FHSS AND FREQUENCY QUORUM RENDEZVOUS

We now present the spread spectrum scheme and frequency hopping algorithm, which is faster and more robust against PHY attacks.

A. Spread Spectrum Scheme Against PHY Attack

Spread spectrum schemes have been actively investigated in terms of the traditional protection provision against jamming. Two known schemes of spread spectrum are Direct Sequence Spread Spectrum (DSSS) and Frequency Hopping Spread Spectrum (FHSS). In FHSS a sender and a receiver synchronously "hop" between shared sequences. When detecting attack on the current channel they "hop" to the next available channels. The efficiency of the FHSS scheme is based on a shared secure key. Establishing a secure key pairing under PHY attacks requires another secure communication.

A solution to break this dependency is to introduce pseudo random frequency hopping (PFH) which is used in connection establishment of Bluetooth. The sender and receiver 'hop' randomly over multiple frequencies and if meeting on the same frequency by chance, they exchange the key. In classical Spread Spectrum techniques (FHSS, DSSS), the sender and receiver share a secret key during communication, where the receiver constructs the random sequence to detect and decode the sender's signal. In SS techniques key exchange between sender and receiver is required. Communicating may be impossible in the presence of a jammer.

There have been several publications to suggest solutions to this problem. In [6], [7] the uncoordinated Spread Spectrum (USS) technique has been developed, which enables anti-jamming communication between nodes, without exchanging the secret key.

FHSS scheme is not efficient in terms of rendezvous latency, and time latency increased under PHY attack. Or in the worst case an attacker may block the rendezvous slot. To improve these vulnerabilities we propose the frequency hopping method.

B. Frequency Quorum Rendezvous

1) Frequency Hopping System

This section presents the Frequency Quorum Rendezvous (FQR) algorithm, which is based on a cyclic quorum system [8]. The FQR exploits two random hopping sequences independently during the key establishment phase. The intersection property of the quorum system, guarantees at least one meeting of pairs of nodes in one time slot [9], where they exchange the key. Assume that time is divided into periods, each of which consists of *t* time slots.

Also suppose that there are *N* available frequencies, $f_i \in \{0,1,\ldots,N-1\}$,

A frequency hopping system is determined by assigning frequencies to time slots in one period. Therefore, a channel hopping sequence A can be represented as follows: $A = \{a_0, a_1, \ldots, a_{t-1}\} = \{(0, f_0), \ldots, (t-1, f_{t-1})\}$,

Where $a_i \in A$ is consisted of a pair of (time slot index, frequency index), and $fi \in \{0,1,\ldots,N-1\}$ represents the frequency index at time slot *i*. Two random frequency hopping sequences A and B rendezvous if they have at least one common element: $a_i = b_i, (0 \le i \le t-1)$. When a pair of nodes (sender, receiver) selects the rendezvous sequences A and B they are on the same frequency at the same time at least once within a period.

2) Quorum System.

A quorum system is a group of quorums of a universal set, where each random pair intersects. Terminologies from [8], [9], [10], and [11] are used to define the details regarding the Quorum system.

Definition 1. Given a finite universal set $U = X_N = \{0,1,\ldots,N-1\}$ of *N* elements, a subset $S = \{a_1, \ldots, a_k\} \subset X_N$, where $a_i \in \{0,1,\ldots,N-1\}$, $k \le N$, presents a cyclic (*N*, *k*) difference set if for every $S \neq 0\ (modN)$ exist at least one pair of elements (a_i, a_j), where $a_i - a_j \equiv S(modN)$. For given *N*, Jiang et al. [8] proved that $\sqrt{N} \le k \le N$. For minimum *k*, the difference set (*N*, *k*) is called minimal (*N*, *k*) difference set.

Definition 2. For (*N*, *k*) difference set $S = \{a_1,\ldots,a_k\} \subset X_N$ a cyclic quorum systems constructed by S is $C = \{Q_0, \ldots, Q_{N-1}\}$, where $Qi = a1+i, a2+i, \ldots, ak+i\ (modN)$ and $i = 0,1,\ldots,N-1$.

C. Frequency Hopping Quorum Rendezvous

Algorithm 1 is the FQR construction algorithm

1. *Input*: *N*, *k*, U=X_N, and quorum system C
2. Sending sequence A and receiving sequence B
3. Select *i* randomly, where $i \in U = \{0,\ldots,N-1\}$
4. Compute a quorum $Q_i = \{q_0, \ldots\ldots, q_{k-1}\}$, where $Q_i \in C = \{Q_0, \ldots, Q_{N-1}\}$
5. *Initials*: A=0, B=0
6. For *j*=0 to k^2-1 do
7. $m \leftarrow j \bmod k$
8. $n \leftarrow \frac{j-(j \bmod k)}{k}$
9. $a_j = (j, q_m), where\ q_m \in Q_i$
10. $b_j = (j, q_n), where\ q_n \in Q_i$
11. $A \leftarrow A \cup a_j$
12. $B \leftarrow B \cup b_j$
13. $end\ for$
14. *Output*: $A = \{a_0, \ldots\ldots, a_{k^2-1}\}$
15. *Output*: $B = \{b_0, \ldots\ldots, b_{k^2-1}\}$

Algorithm 1. FQR algorithm

The algorithm generates two different sequences, sending and receiving, by dividing frequencies to time slots. We present the algorithm with an example: *N*=6, *k*=3, a minimal (*N*, *k*) difference set. The procedure is as follows:

1. Construct a universal set U=X_6={0, . . . ,5} and assume a (6, 3) difference set S, ($\sqrt{6} \le 3 \le 6$).
2. Construct a cyclic quorum system $C = \{Q_0, \ldots, Q_5\}$ from S.
3. A node A selects a random number *i=2* from U and then assign Q_2={2,3,5} from C, e.g. Q_0={0,1,3} [8], Q_1={1,2,4}, Q_2={2,3,5}, Q_3={3,4,0}, Q_4={4,5,1}, Q_5={5,0,2}.
4. The following equation computes frequency to the time slot *j* from the quorum $Q_2 = \{2,3,5\}, = (j, q_m)$, and $b_j = (j, q_n)$, where *m=j mod k, and n=(j-(j mod k))/k*.
5. Repeat step 4 for all k^2=9 time slots, and build sending and receiving sequences.
   Sending sequence:
   S_S={(0,2),(1,3),(2,5),(3,2),(4,3),(5,5),(6,2),(7,3),(8,5)}.
   Receiving sequence:
   R_S={(0,2),(1,2,(2,2),(3,3),(4,3),(5,3),(6,5),(7,5),(8,5)}.
6. In the same manner a node B repeats steps 4 and 5 with a randomly selected quorum $Q_3 = \{3,4,0\}$, and then builds two hopping sequences S_S' and R_S'.
   Sending sequence:
   S_S'={(0,3),(1,4),(2,0),(3,3),(4,4),(5,0),(6,3),(7,4),(8,0)} and
   receiving sequence:
   R_S'={(0,3),(1,3),(2,3),(3,4),(4,4),(5,4),(6,0),(7,0),(8,0)}.

Steps 5, 6 together can be illustrated in Figure 2, where node A is represented with sequence S_S and node B with sequence R_S'. Notice that they rendezvous on channel 3 at time slot 1.

One time period									
Time slot	0	1	2	3	4	5	6	7	8
Node A: S_S of quorum Q_2	2	3	5	2	3	5	2	3	5
Node B: R_S' of quorum Q_3	3	3	3	4	4	4	0	0	0

Figure 2. QRCH with (6,3) difference set.

With FQR algorithm if a node wants to transmit, it hops a frequency according to the sending sequence. On the contrary, the node selects the receiving sequence. The quorum size presents the length of one time period. One time period contains *k* frames, each of which is consisted of *k* time slots, i.e. one time period has k^2 time slots. One period presents the upper bound where FQR ensures at least one rendezvous. FQR exploits the minimal (*N*, *k*) difference set, where the upper bound of time delay for rendezvous is k^2, which also approximates the given number of frequencies *N*. On random hopping channel, *N* is the optimal value.

IV. PHYSICAL LAYER SECURITY

Wireless channels are sensitive to channel jamming, where attackers can easily disturb and suspend legitimate users from accessing a wireless network. This form of attack can disturb traffic, injecting false message into the wireless network. Without better authentication mechanism an attacker can take unauthorized access to a wireless shared medium and destroy all data transmission and security infrastructures. The PHY layer of most wireless systems does not possess a built-in security feature. As a security solution, spread – spectrum modulation techniques are used at the PHY layer to prevent jamming attack. The jamming attack, as a vulnerability of the PHY layer, is treated by security solutions of the PHY layer. All PHY attacks are categorized into four groups: jamming, eavesdropping, restricting access and injecting. In this work we evaluate the performance of the FQR algorithm under jamming attack and restricting access.

A. Jamming Attack

The jammers use many different attack strategies in order to interfere with other wireless communications. These various attacking models will have different levels of effectiveness, and also require different detection strategies.

Jamming presents Denial of Service (DoS) attack that interferes with the communication between nodes. It prevents a legitimate sender or receiver from transmitting or receiving packets on the communication network. A jamming attack continuously emits signals into the shared medium causing interference or fills the wireless medium with noise signals. To perform selective jamming, the adversary must be capable of classifying transmitted packets in real time, and corrupting them before the end of their transmission. [12]. Packet classification can be performed by receiving just a few bytes of a packet, for example, by decoding the frame control field of a MAC-layer frame.

In [13] a power-constrained jammer can corrupt a small number of data bits, which leads to the loss of the entire packet. A jammer can also block data transmission by continuously injecting noise-like signals (or dummy packets) into a wireless channel, namely a PHY-layer attack [14]. According to objectives and strategies the jammers are classified into several categories:

Proactive jammer emits noise signals continuously to completely block a wireless channel and due to this behavior can easily be detected.

Reactive jammer listens to the channel first and launches a jamming attack only if sensing any signals on the channel.

B. Restricting Access

This type of attack tries to destroy the MAC protocol in order to prevent the legitimate nodes from initiating MAC operation or causing packet collision. This conceptually can approximate with reactive jamming, which starts an attack when sensing any signal on the channel. But the targets of this access attack are a multi-user access procedure. Another form of restricting access is the form in which the attacker backs off its timer very short so that it occupies the wireless shared medium first all the time. The others privileged nodes will sense these signals in the channel and postpone their transmission. These forms of attack can approximate with proactive jammer.

C. Attack Model

We suppose that a jamming attack fills the wireless medium with noise signals on a subset of different frequencies (channels) n_b, and block all those frequencies. At the same time, it can listen to other frequencies n_s for ongoing transmission. Also assume that a smart jammer does not listen and block the same frequency at the same time, meaning $n_b \cap n_s$=0. From restricting access also assume that n_m frequencies (nodes) are prevented to initiate MAC operation and n_{sh} other frequencies (nodes) are restricted from access as a result of a short backoff timer. Then for the total number of available frequencies N in a network, we have $N = n_b + n_s + \mathrm{n_m} + \mathrm{n_{sh}} + n_c$, where n_b, n_s, $\mathrm{n_m}$, $\mathrm{n_{sh}}$, n_c, is the number of blocked frequencies, number of sensed frequencies, number of prevented frequencies for MAC operation, number of prevented frequencies from the short timer and the number of clear frequencies respectively. Thus the number of attacked frequencies n_j presents the total number of frequencies that are being blocked or are possibly blocked after being sensed or restricted from access i.e. $n_j = n_b + n_s + \mathrm{n_m} + \mathrm{n_{sh}}, (0 < n_j < N)$. Then the probability of PHY attack P_j is given by $P_j = {}^{n_j}/_{N}$.

D. Key Establishment Under PHY Attack

Key establishment protocol relies under attack resistant and requires the available of a shared secret key. Through the proposed FQR algorithm, a pair of nodes transmit-receive message and under the presence of attacker, such the key pairing must be established securely.

If the nodes get their public-key certificates issued by a trusted authority, they still need to communicate in order to establish the secret key via an authentication Diffie – Hellman (DH) protocol [15]. Under DH authentication scheme, two nodes exchange message with public key and encrypted key. Because the message *M* does not fit in one transmission slot, it can split into the *l* fragments (*M1, M2, . . . , Ml*) each of which can fit into one time slot.

In order for FQR to resist a jamming attack, the *dwell* time on the frequency channel must be short. The message *M* is split into a set of short fragment *M1, . . . ,Ml*, which a typical size is only a few hundred bits. Such a short slot time duration can prevent detection by jammers with significant probability.

In [16] is explained that a node can send and receive packets simultaneously. A node continuously sends the set of *l* packets and in parallel receives the incoming packets. After receiving the *l* packets from A[1], *B* validates A's signature, if certified, $B_{(MA)}$ transmits its signature to $A_{(MB)}$. A terminates sending the packets set when a timeout expires or A verifies B. According these, for DH authentication is necessary successful transmission of *2l* packets. After authentication, A and B extract the shared key from which they construct a common hopping sequence. Then they transmit data hopping along the

[1] A is a sender and B is a receiver

same frequency. As have explained before, that nodes are needed to exchange *2l* packets for authentication, the next issue is transmission of packets in the presence of jammers. The nodes can transmit packets, when they rendezvous. The FQR algorithm can provide at least one rendezvous within one period of k^2 time slots.

V. EVALUATION

In order to evaluate the FQR algorithm, we apply MATLAB for the cyclic quorum system by using the minimal (*N*, *k*) difference set (for different values of N, the value of k can be read from the Table in [8]). For the purpose of performance measuring, we provide a comparative analysis by presenting the random hopping (RH) scheme, where a pair of nodes hops at the same speed. We assume that the hopping speed of a sender is f=2,4 KHz, the duration of a time slot (*dwell time*) is $\delta = 417\ \mu s$, and the switching latency is $\tau = 70\ \mu s$. The network bandwidth is B=2 Mb/s and the length of the messages is L=1600 bits. This length is split into set of *l*=8 packets. Thus, transmission time of a packets will be $t_p = {}^{L}/_{l} / B = 100\mu s < \delta$. Additionally, we evaluate the performance under jamming attack and restricting access (PHY attack) by considering the DH protocol as a key establishment protocol.
This experiment evaluates two metrics: Time latency [time slot] without attack as an average time for nodes to Rendezvous, and the time latency under PHY attack.

A. Experiments and Results

As far as the first experiment is concerned, we investigated the impact of the time latency (slots) on transmitting *2l* packets with P_j=0 from the number of available frequencies (*N*), which can be computed with the following expression, $t_{2l} = 2l(\delta + \tau)N\ [s]$, or expressed in time slots will be: $t_{2l} = 2l\frac{\delta+\tau}{\delta}N\ [time\ slot]$. The FQR scheme reduces these time slots for the factor $({}^{N}/_{k^2})$ i.e., $t_{2l,Q} = 2l\frac{\delta+\tau}{\tau}N\ \frac{N}{k^2}\ [time\ slot]$. In Figure 3, these impacts are presented as values of time latency (time slots). According to this Figure, we notice that in terms of time latency, the FQR algorithm shows better performance compared to RH. Moreover, the difference of time latency increases as *N* increases, and when *N*=100, the FQR algorithm reduces the time latency approximately for 30 percent.
In the next experiment, we investigated the impact of time latency on the performance of a FQR scheme with the probability of PHY attack in a wireless network, having 100 potentials channels. P_j is defined as probability of PHY attack on any time slot, given as $P_j = n_j/N$, where n_j is the number of jammed frequencies, whereas *N* is the number of available frequencies. P_j indicates that any transmitted packet in the wireless network has been attacked. The equation P_j=0 indicates that there is no attack. The expression for time latency can take the form as follows: $t_{2l,Q}(P_j)|_{N=100} = \frac{t_{2l,Q}}{1-P_j}$. And $t_{2l}(P_j)|_{N=100} = \frac{t_{2l,Q}(P_j)}{{N_c}/{K_c^2}}$, where N_c presents the rested clear number of frequencies i.e., $N_c = N(1 - P_j)$, and K_c is the corresponding factor of the minimal difference set (N_c, K_c).
Figure 4 presents the impact of time latency with the probability of PHY attack. FQR algorithm shows better performance compared to RH in terms of time latency. Obviously, the FQR reduces the time latency, and for higher probability values, P_j=0.9, the reduction is approximately 35 percent.

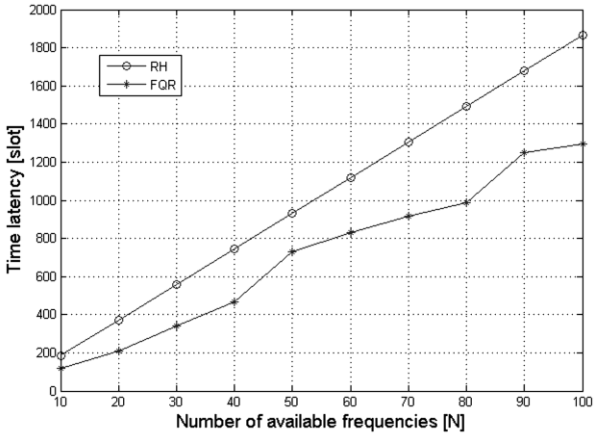

Figure 3. The impact of time latency of frequency hopping algorithm with varying number of available frequencies.

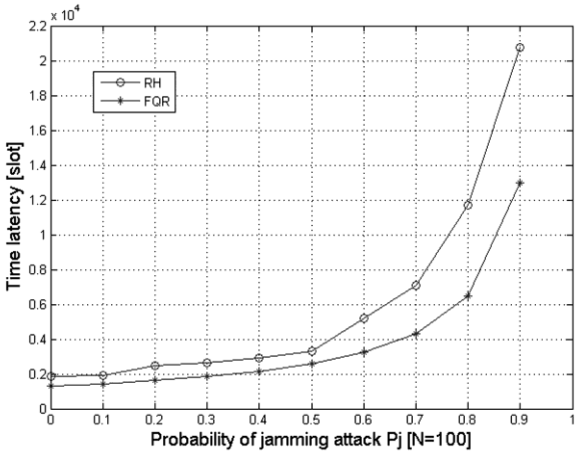

Figure 4. Impact of time latency of frequency hopping algorithm with the probability of PHY attack P_j, (*N*=100).

VI. CONCLUSION

In this work we propose the implementation of FQR algorithm in wireless smart grid communication. The PHY layer is the lowest level of multiple layers wireless network architecture. This architecture will satisfy requirements of smart grid applications in large scale. The attack against PHY layer is the challenges of all architecture.
The proposed FQR scheme for anti-jamming communication is faster and robust compared to previous RH scheme. This scheme constructs two different sequences and allows nodes to hop over random multiple frequencies without any pre-

defined sequence, which provide secure communication. The FQR system provides Rendezvous amongst nodes within a bounded time, which reduces the time latency.

REFERENCES

[1] C. L. Philip Chen. Jing Liu and Xiao, Shuhui Li, Wei Liang, "Cyber Security and privacy Issues In Smart Grids," *IEEE Communication surveys & tutorials, IEEE*, vol. 14, no. 4, 2012, pp. 981 – 997.

[2] E.-K. Lee, S. Y. Oh, and M. Gerla, "Fast and Resilient Key Establishment Using Quorum Rendezvous Under Jamming Attack," Technical report 11005, UCLA, 2011.

[3] K. Bian, J.-M. Park, and R. Chen, " A Quorum-Based Framework for Establishing Control Channels in Dynamic Spectrum Access Networks," in *Proc. ACM* at *the 15th Annual International Conference on Mobile Computing and Networking*, 2009, pp. 25-36.

[4] NIST "Framework and Roadmap for Smart Grid Interoperability Standards," Release 2.0, NIST Special Publication 1108R2, February 2012.

[5] J. C. L. Cheung, T. W. Chim, S. M. Yiu, L. C. K. Hui, and V. O. K. Li, "Credential-Based Privacy-Preserving Power Request Scheme for Smart Grid Network," *Proc. IEEE Global Telecommunications Conference - GLOBECOM 2011*, Dec. 2011, pp. 1–51.

[6] M. Strasser, C. Pöpper, and S. Čapkun, "Efficient Uncoordinated FHSS Anti-Jamming Communication," *Proceedings of the Tenth ACM International Symposium on Mobile Ad Hoc Networking and Computing - MobiHoc '09*, 2009, p. 207-218.

[7] M. Strasser, C. P, S. Capkun, and M. Cagalj, "Jamming-Resistant Key Establishment Using Uncoordinated Frequency Hopping," *2008 IEEE Symposium on Security and Privacy (sp 2008)*, May 2008, pp. 64–78.

[8] W. -S. Luk and T. -T. Wong, "Two New Quorum Based Algorithms for Distributed Mutual Exclusion," *Proceedings of 17th International Conference on Distributed Computing Systems*, 1997, pp. 100–106.

[9] E.-K. Lee, S. Y. Oh, and M. Gerla, "Physical Layer Security in Wireless Smart Gid," *IEEE Communication Magazine*, vol. 50, no. 8, 2012, pp. 46–52.

[10] J. Jiang, Y. Tseng, C. Hsu, and T. Lai, "Quorum-Based Asynchronous Power-Saving Protocols for IEEE 802.11 Ad Hoc Networks," *Mobile Networks and Applications*, 2005, pp. 169–181.

[11] P. Hartel, J. Den Hartog, and P. Havinga, "Link-Layer Jamming Attacks on S-MAC," *Proceeedings of the Second European Workshop on Wireless Sensor Networks, 2005*, pp. 217–225.

[12] M. G. Divya. S, "Jamming Attack Prevention in Wireless Networks Using Packet Hiding Metods," *IOSR Journal of Computer Enginering (IOSRJCE)*, 2012.

[13] G. Lin, "Poster : Low-Power DoS Attacks in Data Wireless LANs and Countermeasures Categories and Subject Descriptors," 2003.

[14] W. Xu, W. Trappe, Y. Zhang, and T. Wood, "The Feasibility of Launching and Detecting Jamming Attacks in Wireless Networks," *Proceedings of the 6th ACM international symposium on Mobile Ad Hoc Networking and Computing - MobiHoc '05*, 2005, pp. 46-57.

[15] American National Standards Institute "Key Agreement and key transport using elliptical curve cryptography". Technical report, A.X9.63-2001, 2001.

[16] C. Popper, M. Strasser, and S. Capkun, "Anti-Jamming Broadcast Communication Using Uncoordinated Spread Spectrum Techniques," *IEEE Journal in Selected Areas in Communication Special Issues on Mission Critical Networking*, vol. 28, no. 5, 2010, pp. 1–13.

Halim Halimi is currently working toward a Ph.D degree in the Faculty of Electrical Engineering and Information Technologies at the Ss. Cyril and Methodius University of Skopje, Macedonia. He is currently a research assistant with State University of Tetovo, Tetovo, Macedonia. His research interests include smart grid security, applied cryptography.