A Secure Cognitive Radio Ad-Hoc Network with the Capability of SSDF Attack Detection

Rashin Saboor, Ali Payandeh, and Hojatolah Rohi

Abstract—**In this article, we made an attempt to clarify it that the inadequacy problem of required spectrum for the exchanges presented in MANET can be solved by means of the Cognitive radio network since it has the sensing potentiality of their surrounding environment and can access to a supplementary frequency band via their parameters comparison. Key management and authentication are two important factors in MANET security. The recent development in Identity-based cryptography has made this method a potential candidate for MANET. However the security in CR-MANET has attracted less attention in comparison with other regions. The authors try to propose an Identity-based cryptography with threshold secret sharing which has been designed for MANET security especially; this method will result in the elimination of SSDF attack trouble in Cognitive radio Ad-Hoc Networks, where the intruder sends wrong results of local spectrum sensing and leads to a wrong spectrum sensing determination in cognitive radios consequently. Following cooperative spectrum sensing scheme, it can find out SSDF attack occurrence, limit intruders' access to t neighbor nodes for the key updating or delete the intruder nodes from the network.**

Index Terms—**Cognitive radio, IBC, MANET, SSDF attack.**

I. Introduction

The current progress of communication networks has caused the emerge of wireless Ad-Hoc networks as self-organized ones that can be formed with no infrastructure. The Ad-Hoc networks have a wide capability for supporting and covering different wireless standards. Although its current application is severely bound to ISM band (900MHz to 240GHz). The wireless devices development has made the wireless bands to be intensively filled. There are several licensed bands such as 400MHz to 700MHz ranges accessible for operators which are occasionally used. FCC has set forth a scheme to eliminate the mentioned spectrum deficiency and to make available licensed bands for devices exist in unlicensed ones. This new research area has caused CR networks progress. Unlicensed users named as cognitive radio or secondary users, are obliged to empty the band as soon as they face licensed or primary users. The cognitive radio enables the usage of temporarily unused

Spectrum, which is referred to as spectrum hole or white space. If this band is further utilized by a licensed user, the cognitive radio moves to another spectrum hole or stays in the same band, altering its transmission power level or modulation scheme to avoid interference.

Cognitive radio (CR) networks can be classified as the infrastructure-based CR network and the CRAHNs [1]. Since CRAHNs has no infrastructure, a CR user can communicate with other CR users through ad hoc connection on both licensed and unlicensed spectrum bands.

The cooperative scheme investigated in [2] is necessary because a CR user in CRAHNs can-not foresee his behavior's effect on all the networks merely on the basis of local observations. In addition, the spectrum sensing is a key factor in CR, for it avoids harmful interference with licensed user and finds existing spectrum holes for the CRs. It's not possible for all the CRs to experience receiver uncertainty or fading altogether because of the place or local differences so if the majority of users observe a primary user, they will be able to share their results. Consequently, the overall detection performance can be greatly improved. The cooperation among CR users raises new concerns for the reliability and the security in cooperative sensing. This is because, when multiple CR users cooperate in sensing, a few CR users who report unreliable or falsified sensing data can easily influence the cooperative decision.

Two known security threats in CRs are incumbent (IE) and spectrum sensing data falsification (SSDF).

In [3]-[5] some techniques have been mentioned to recognize SSDF attack occurrence. In this article we present a cooperative spectrum sensing scheme based on threshold and Identity- based cryptography parameters which can-not only recognize SSDF attack occurrence but also find an intruder and delete him from network or at least harden his access to the t- number of neighbors key.

II. Key Management and Authentication in Manet

Mobile AD-Hoc networks encounter with much more security problems in comparison with wired networks for some reasons like the lack of a network infrastructure or dynamic topology of the network and also wireless link damages. Common security techniques are usually effective for several security threats while they are not proper enough for a combination of former ones. Cryptography is then used to provide a general design framework. Cryptography techniques used in MANETs can be classified into two categories, namely, Symmetric Key based and Asymmetric Key based. In symmetric key based schemes, if an attacker compromises the symmetric key of a group of users, then all encrypted messages for that group will be exposed. Asymmetric key schemes have more functionalities than

Manuscript received February 14, 2013; revised April 12, 2013. This work was supported in part by Iran Telecommunication Research Center.

R. Saboor is with the University of MUT, Tehran, Iran (e-mail: rashin.saboor@gmail.com).

A. Payandeh is with the Iran Telecommunication Research Center (CSRI), Tehran, Iran (e-mail: payandeh@mut.ac.ir).

H. Rohi is with the Electrical Engineering Department, Malek ashtar University of Technology, Tehran, Iran (e-mail: hh_rohi@yahoo.com).

DOI: 10.7763/IJFCC.2013.V2.245

symmetric ones, e.g., key distribution is much easier, authentication and non-repudiation are available, and compromise of a private key of a user does not reveal messages encrypted for other users in the group. However, they are computationally expensive. Asymmetric cryptography is usually based on PKI. Since PKI success is bounded to a CA[1] which has a central control unit, it is not proper for MANET.

A. Application of IBC in MANET

IBC[2] is a special form of a PKI cryptography considered as an asymmetric cryptography. The idea of IBC was first proposed by Shamir [6] in 1984. Shamir introduced a novel type of cryptographic scheme, which enables any pair of users to communicate securely and to verify each other's signatures without exchanging private or public keys, without keeping key directories: and without using the services of a third party. Such a scheme has the property that a user's public key is an easily calculated function of his identity, while a user's private key can be calculated for him by a trusted authority, called a Private Key Generator (PKG). The application of IBC in MANET was proposed as a significant research subject for it doesn't require issuing licenses and public keys. Later some other schemes of IBC based on Weil pairing in elliptic curves were presented in [7], [8]. So it is also called as pairing- based cryptography.

B. Threshold Cryptography and Key Management in MANETs

Most of the Identity-based cryptography systems apply Shamir threshold cryptography [6] in which they contribute a secret quantity among a number of users. Shamir explains how to divide D to *n*-parts in such a way it can be easily reconstructed from *t*-parts, and even in the case of being completely informed about *t*-1 parts, D still remains secret and not any information reveals about it.

Shamir proposes a (*t*, *n*) threshold scheme to solve this problem based on polynomial interpolation. He suggests picking a random *t* − 1 degree polynomial $q(x) = a_0 + a_1 x + ... + a_{t-1} x^{t-1}$ in which $a_0 = D$, and each piece is the value of the polynomial at the n points. Thus any subset of t of the pieces can determine the coefficients of the polynomial (using e.g. Lagrange interpolation) and thus the secret data at a certain point.

III. (T, N) Threshold and Identity-Based Key Management

The idea of distributed CA has been subsequently adopted for distributed PKG in many IBC proposals in MANETs later. Khalili [9] suggested to apply IBC for a secure AD-Hoc network and create a mechanism for an effective key distribution in MANET with contribution of both IBC and threshold cryptography techniques. References [10], [11] presented fit and proper schemes on the mentioned subject too. All methods deal with application of IBC in MANET have been investigated in [12].

The proposed approach in [13] comprises of two components: Distributed key generation and identity-based authentication. The key generation component provides the network master key pair and the public/private key pair to each node in a distribute way. The generated private keys are used for authentication. Identity-based authentication mechanism provides end-to-end authentication and confidentiality between the communication nodes.

A. Master Key Generation

The master key pair is computed collaboratively by the initial network nodes without constructing the master private key at any single node. The scheme we used [11] is an extension to Shamir's secret sharing [8] without the support of a trust authority. In the scheme, each node *Ci* randomly chooses a secret xi and a polynomial $f_i(z)$ over GF(q) of degree t-1, such that $f_i(0) = x_i$. Node Ci computes his sub-share for node Cj as $SS_{ij} = f_i(j)$ for j=1,…n and sends SS_{ij} securely to Cj. After sending the n-1 sub-shares, node Cj can computes its share of master private key $S_j = \sum_{i=1}^{n} SS_{ij} = \sum_{i=1}^{n} f_i(j)$. That is, the master key share of node C_j is combined by the sub-shares from all the nodes, and each of them contributes one piece of that information. Similarly, any coalition of *t* shareholders can jointly recover the secret as in basic secret sharing using $\sum_{i=1}^{t} S_i . l_i(z) \bmod(q)$, where l_i (*z*) is the Lagrange coefficient. It is easy to see that the jointly generated Master private key $Skm = \sum_{i=1}^{n} x_i = \sum_{i=1}^{n} f_i(0)$.

After the master private key is shared, each Shareholder publishes S_iP, where *P* is a common parameter used by the identity-based scheme. Then the master public key can be computed as $QM = \sum_{i=1}^{n} S_i . P$

B. Distributed Private Key Generation

Using the identity-based cryptography, a mobile node's public key can be any arbitrary string. In our scheme, the public key is computed as QID = H(ID|| Expire _ time) where H() stands for a hash function defined in identity-based encryption [8], ID represents the identity of the node, and Expire_time is a time stamp protecting from the private key loss. The nodes also need to obtain their corresponding private keys. The way to obtain the private key is to contact at least t neighbor nodes, present the identity and request private key generation (PKG) service. Each of the t PKG service nodes generates a secret share of a new private key sk and sends to the requesting node. The process of generation of a share of the new secret key sk can be represented by ski = SiQID, where Si (i=1,…, t) is the share of the master private key of the serving node, ID is the identity of the requesting node, QID is its public key, and ski denotes the generated private key share for the requesting node. By collecting the t shares of its new private key, the requesting node would compute its new private key $Sk = \sum_{i=1}^{t} S_i . QID$.

[1] Certificate Authority

[2] Identity- based cryptography

IV. Spectrum Sensing for Cognitive Radio Ad Hoc Networks

The components of the cognitive radio ad hoc network (CRAHN) architecture can be classified in two groups as the primary network and the CR network components. The primary network is referred to as an existing network, where the primary users (PUs) have a license to operate in a certain spectrum band. Due to their priority in spectrum access, the PUs should not be affected by unlicensed users. CR users are mobile and can communicate with each other in a multi-hop manner on both licensed and unlicensed spectrum bands. Usually, CR networks are assumed to function as stand-alone networks, which do not have direct communication channels with the primary networks. Thus, every action in CR networks depends on their local observations. In order to adapt to dynamic spectrum environment, the CRAHN necessitates the spectrum-aware operations. The objectives of spectrum sensing are twofold: first, CR users should not cause harmful interference to PUs by either switching to an available band or limiting its interference with PUs at an acceptable level and, second, CR users should efficiently identify and exploit the spectrum holes for required throughput and quality of service (QoS).

A. Cooperative Spectrum Sensing

Many factors in practice such as multipath fading, shadowing, and the receiver uncertainty problem [1] may significantly compromise the detection performance in spectrum sensing. However, due to spatial diversity, it is unlikely for all spatially distributed CR users in a CR network to concurrently experience the fading or receiver uncertainty problem. If CR users, most of which observe a strong PU signal can cooperate and share the sensing results with other users, the combined cooperative decision derived from the spatially collected observations can overcome the deficiency of individual observations at each CR user. Thus, the overall detection performance can be greatly improved [2].

If the sensing time can be reduced due to cooperation, CR users will have more time for data transmission so as to improve their throughput.

The process of cooperative sensing starts with spectrum sensing performed individually at each CR user called local sensing. Typically, local sensing for primary signal detection can be formulated as a binary hypothesis problem as follows [14]:

$$x(t) = \begin{cases} n(t), & H_0 \\ h(t).s(t) + n(t), & H_1 \end{cases} \tag{1}$$

where $x(t)$ denotes the received signal at the CR user, $s(t)$is the transmitted PU signal, $h(t)$ is the channel gain of the sensing channel, $n(t)$ is the zero-mean additive white Gaussian noise (AWGN), H0 and H1 denote the hypothesis of the absence and the presence, respectively, of the PU signal in the frequency band of interest.

V. SSDF Attack Models in Cooperative Spectrum Sensing Schemes

In cooperative spectrum sensing, malicious secondary users may launch SSDF attacks by sending false local spectrum sensing results to others, resulting in a wrong spectrum sensing decision. Three attack models are presented as follows [13].

In the first attack model, a malicious secondary user sends out relatively high primary user energy to indicate the presence of primary users although there is no primary user and its sensed energy is low. In this case, other secondary users make a wrong decision that primary users are present and they will not use the spectrum. The intention of the malicious secondary user is to gain the exclusive access to the target spectrum. We call this kind of attacks as selfish SSDF. In the second attack model, a malicious secondary user sends out relatively low primary user energy to indicate the absence of primary users although there are primary users and its sensed energy is high. In this case, other secondary users make a wrong decision that there is no primary user and they will use the spectrum. The intention of the malicious secondary user is to give interference to primary users. We call this kind of attacks as interference SSDF. In the third attack model, a malicious secondary user sends out random primary user energy during the process of cooperative spectrum sensing. The intention of the malicious secondary user is to make other secondary confused, and no consensus can be reached among secondary users. We call this kind of attacks as confusing SSDF.

VI. The Proposed Scheme for SSDF Attack Detection, Based on Identity-Based and Threshold Cryptography

In network formation phase, as an elementary part required for algorithm, network public and private keys based on their identity and applying the current algorithm in [8] are obtained for all nodes one by one and try to avoid the entrance of users have no valid ID to the network. Then a matrix is made inside each one of the nodes as Table I. To accomplish primary exchanges of (t, n) threshold key management pattern based on identity and former algorithm phases of sensing data exchanges, a common default control channel is used. 16 licensed channels can be created in accordance with spectrum sensing operation if IEEE 802.11 is used.

A. The first phase

- Every CR user senses by himself his surrounding environment in a pre-defined due time. He specifies digit 1 for channels occupied by primary users and digit 0 for empty channels and save a 16 bit -string.
- The string encrypts with the node's private key obtained via ID-based threshold cryptography. Then the encrypted string attaches to the node ID which can be a 64 or 128 bit –string, and broadcast for its one-hop neighbors finally.
- Receiver nodes don't need to get the node public key but they can make it themselves regarding to the node sender's ID and encrypt the transmitted 16-bit- string.
- Each node has to receive at least, t-string, from its neighbors to be permitted to enter in cooperative spectrum sensing. Otherwise it is to move for finding more neighbors in a due time.

- Receiving its neighbors-strings, the node XOR the strings separately with its local sensing data and record the result in front of the neighbor's node-ID (NID).
- If the recorded string against a node-ID is opposite zero, namely two nodes have different sensing results, so an intrusion detection bit against the node will be 1 and at the same time the counter against each node will increase one digit for a sole neighbor.

B. The Second Phase

- Every node concatenates and encrypts the ID of nodes with different sensing results, and then sends the resulted string for its neighbors.
- The number of times each node receives another node ID for the cause of uniformity with its neighbors sensing string will be added to the counter against the node in Table I.
- There is a Revocation Key Counter (RKC) for a node against each NID.

TABLE I: INTERNAL DATA STRUCTURE OF NODES

Node	ID_1	$counter(i,1)$	…	ID_N	$counter(i,N)$
ID_i					

C. Decision Phase

- If the counter against each node is equal or bigger than [*t*/2], one digit will be added to the RKC counter and the transmitted sensing results obtained from the node will be abandoned. Considering "*t* out of *N*" rule, this section is fulfilled on the neighbors' t-node not the whole network ([*t*/2] out of t). This quantity of threshold may also be utilized instead of [3*t*/4] and [*t*/3].
- After doing binary OR operation on the received string of the nodes where RKC is less than [*t*/2], the resulting string will be saved inside each node. If even one single channel is found occupied, it should be considered to avoid interference.

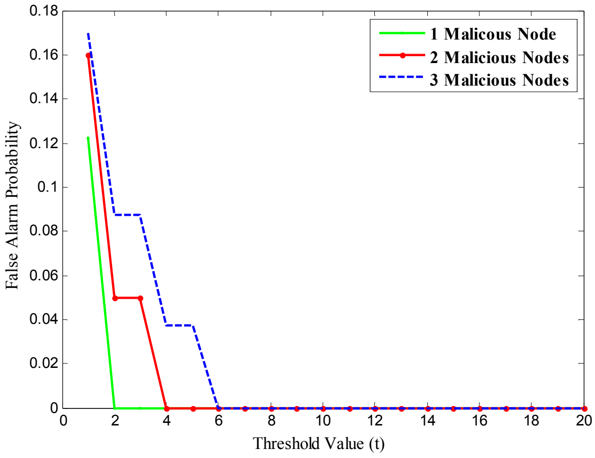

Fig. 1. False alarm probability versus threshold value for various numbers of malicious nodes

- The results obtained from empty channels are used for data transmission.
- In the next sensing phase, if the preceding process is enforced and a node from the same former nodes with an RKC equals 1 and -in one unit-increment (RKC=2), the neighboring node itself can delete the intruder's ID with all rows and columns relating to the node's NID.
- Total key updating process is accomplished.
- Now the intruder node can't be approved by all the network nodes any more. So it is to be deleted instead of a proper threshold of *t*; otherwise it will face a trouble in obtaining *t*-share of *t*-PKG services.

VII. SIMULATION RESULTS AND DISCUSSIONS

The simulation region is a bounded area of 1000×1000 square meters. Nodes are initially placed randomly in this region. The nodes would start moving from their initial position towards a destination and speed values are generated in a random fashion.

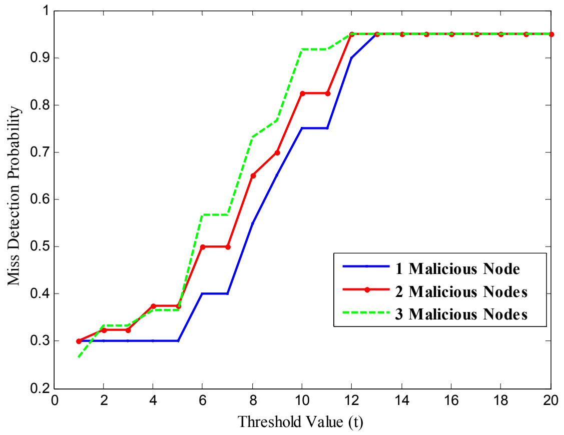

Fig. 2. Miss Detection probability versus threshold value for various numbers of malicious nodes

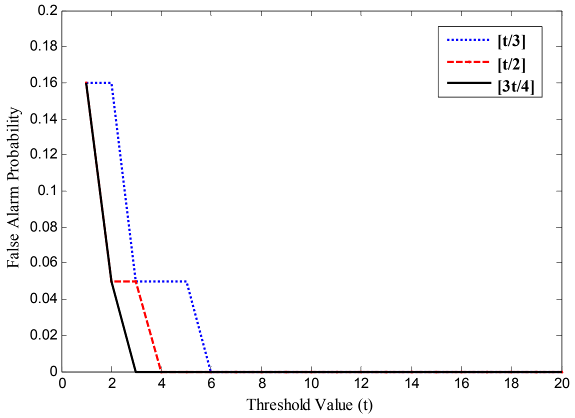

Fig. 3. False alarm probability versus threshold value for different decision levels

The initial transmission range for all communication is assumed to be 400m. The detection performance can be primarily determined on the basis of two metrics: probability of false alarm, which denotes the probability of a CR user declaring that a PU is present when the spectrum is actually free and probability of detection, which denotes the probability of a CR user declaring that a PU is present when the spectrum is indeed occupied by the PU.

Since a miss in the detection will cause the interference with the PU and a false alarm will reduce the spectral efficiency, it is usually required for optimal detection performance that the probability of detection is maximized subject to the constraint of the probability of false alarm.

The simulations are based on a MANET with 20 CRs, in which there are a variety of authentic nodes and malicious attackers. We compare the proposed scheme in all of the following three cases: one attack, two attacks and three attacks.

By varying the value of threshold *t* from 1 to 20, we evaluate the simulations for each *t*, to obtain the optimum performance point of the proposed algorithm.

In threshold cryptography, the large threshold value will lead to harder compromise with *t* number of nodes and greater security. But the amount of computation increases. However, in some situation, the requesting node only has a few neighbors, i.e., it cannot get enough number of shares.

We count this situation as an unsuccessful PKG service. That means, when we vary the value of threshold from low to high, more and more mobile nodes could not get enough number of neighbors for PKG service. Thus, choosing an appropriate threshold value for different network size is important in the real network applications. Different decision levels, such as [*t*/3], [*t*/2] and [3*t*/4] will affect on the results of the proposed cooperative spectrum sensing scheme.

VIII. False Alarm Probabilities and Miss Detection Probabilities

Before presenting the simulation results, we discuss briefly the relationship between Pm (probability of miss detection) =1-Pd (probability of detection) and Pf (probability of false alarm). A High Pm will result in the miss detection of primary users with high probability, which in turn increases the interference to primary users. On the other hand, a high Pf will result in low spectrum utilization since false alarms increase the number of missed opportunities (white spaces). In the first attack, user *M*1 is compromised and sends out falsified data. In the second attack, both users *M*1 and *M*2 are compromised, they send out similar falsified data and in the third attack, users *M*1, *M*2 and *M*3 send out similar falsified data. Fig. 1 shows the results in terms of false alarm probabilities, and Fig. 2 shows the results in terms of miss detection probabilities.

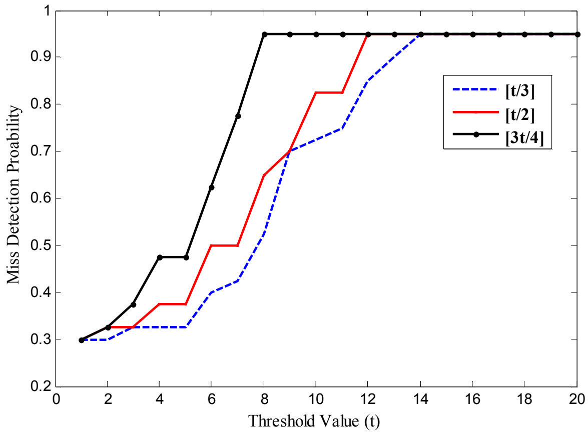

Fig. 4. Miss detection probability versus threshold value for different decision levels

By increasing the number of compromised malicious nodes, correlation between their falsified data can affect on the false alarm and miss detection probabilities.

From Fig. 1, we can see that just in *t*=1, the false alarm probability of the first attack is not zero. When there are more malicious nodes in the network, the false alarm probability increases. But with the increasing number of threshold t, false alarm probability decreases and miss detection probability increases.

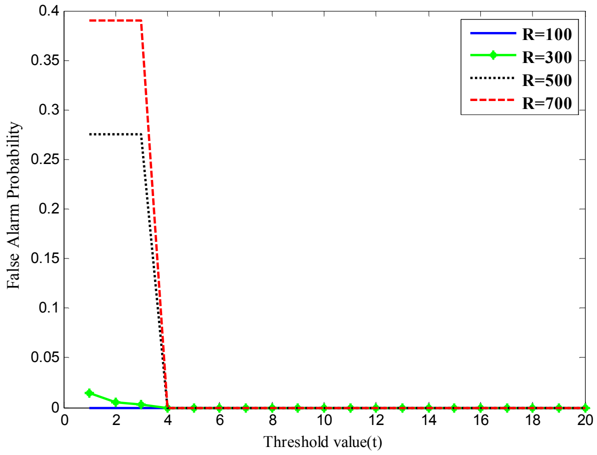

Fig. 5. False alarm probability versus threshold value for different transmission ranges

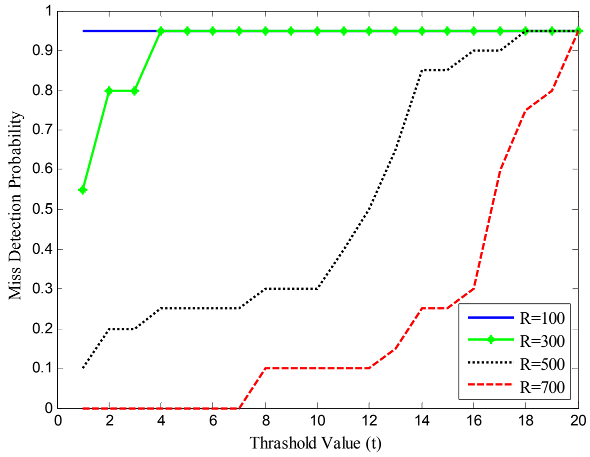

Fig. 6. Miss detection probability versus threshold value for different transmission ranges

From Fig. 3 and Fig. 4, we can see that by increasing the decision levels, false alarm probability decreases and miss detection probability increases and From Fig. 5, and Fig. 6 we can see that, by increasing the transmission range, the miss detection probability decreases but false alarm probability increases, so there is a tradeoff between the detection performance and transmission range of each node during the broadcast process.

IX. Conclusion

The area of security in CR-MANETs has received far less attention than other areas. Malicious CRs can send false local spectrum sensing results in cooperative spectrum sensing. In this paper, according to an Identity-based threshold key management for MANET, we have presented a cooperative spectrum sensing scheme to counter SSDF attacks in CR-MANETs. Through the suggested scheme both SSDF attack and intruder nodes can be diagnosed with an accurate probability. By the way it doesn’t require frequent repetition and long convergence time needed for consensus – based schemes. It causes the network security, confidentiality and authentication as well and finds and discharges intruders from the network. To show current channels status, binary strings are used instead of correspondent signals transmission with different distributions. This procedure decreases the utilization of common control channel, delay and energy consumption too. Moreover, a common receiver is not needed for the final decision in the proposed scheme. It's enforced on the neighboring t nodes instead of the whole network. In the case of the network node increment, the internal calculation of each node limited to its neighboring t-number is still remained. Consequently it's a scalable network.

Future work is in progress to detect other known security threats in CRs to improve the quality of service and security in CR-MANETs.

Acknowledgment

The support of Iran Telecommunication Research Center for this work which is a result of a M.Sc. thesis in Malek ashtar University of Technology is gratefully acknowledged.

References

[1] I. F. Akyildiz, W.-Y. Lee, M. C. Vuran, and M. Shantidev, "NeXt generation/Dynamic spectrum access/cognitive radio wireless networks: a Survey," *Computer Networks Journal* (Elsevier), pp. 2127–2159, 2006.

[2] I. F. Akyildiz, B. F. Lo, and R. Balakrishnan, "Cooperative spectrum sensing in cognitive radio networks: A survey," *Journal of Physical Communication*, vol. 4, pp. 40-62, March 2011.

[3] M. Kim, H. Choo, and M. Y. Chung, "A test framework for secure distributed spectrum sensing in cognitive radio networks," Springer Berlin Heidelberg, pp. 382-391, 2011.

[4] M. Abdelhakim, J. Ren, T. T. Li, "Reliable cooperative sensing in cognitive networks," Springer Berlin Heidelberg, pp. 206-217, 2012.

[5] C. S. Hyder, B. Grebur, and L. Xiao, "Defense against spectrum sensing data falsification attacks in cognitive radio networks," *Secure Comm*, London, Springer Berlin Heidelberg, pp. 154-171, 2012.

[6] A. Shamir, "Identity-based cryptosystems and signature schemes," in *Proc. Crypto 1984*, 1984.

[7] A. Joux, "A one round protocol for tripartite diffie-hellman," *ANTS IV, ser. LNCS*, vol. 1838. Springer-Verlag, pp. 385–394, 2000.

[8] Boneh and Franklin, "Identity-based encryption from the weil pairing," in *Proc. Crypto 2001, ser. LNCS*, vol. 2139. Springer, pp. 213– 219, 2001.

[9] A. Khalili, J. Katz, and W. A. Arbaugh, "Toward secure key distribution in truly ad-hoc networks," *SAINT Workshops*, *IEEE Computer Society*, 2003, pp. 342–346.

[10] W. A. Xiong and B. Tang, "A secure and highly efficient key management scheme for MANET," *Advances on Information Sciences and Service Sciences*, vol. 3, no. 2, March 2011.

[11] H. M. Deng, A. Mukherjee, and D. P. Agrawal, "Threshold and identity-based key management and authentication for wireless Ad Hoc networks," *IEEE Computer Society*, 2004.

[12] S. S. Zhao, A. Aggarwal, R. Frost, and X. L. Bai, "A survey of applications of identity-based cryptography in mobile Ad-Hoc networks," *IEEE Communications Surveys & Tutorials*, vol. 14, no. 2, second quarter 2012.

[13] H. Tang, F. R. Yu, M. Huang, and Z. Li, "Distributed consensus-based security mechanisms in cognitive radio mobile ad hoc networks," *IET Communications*, vol. 6, no. 8, pp. 974–983, 22 May 2012.

[14] I. F. Akyildiz, W.-Y. Lee, and K. R. Chowdhury, "CRAHNs: cognitive radio ad hoc networks, Ad Hoc Networks," pp. 810–8367, 2009.

Rashin Saboor received the B.S. degree in electronics and electrical engineering from Shariaty College, Tehran, Iran in 2008. She is working toward the M.S. Degree in Electrical and Secure Communication Engineering with Mobile Ad-Hoc Networking Laboratory, School of Information and Communication Technology, Malek ashtar University of Technology, Tehran, Iran. Her areas of research include Mobile Ad-Hoc Networks, Cognitive Radio Networks, and cryptography.

Ali Payandeh received the B.S., M.S., and Ph.D. degrees in electronics and communication engineering from K. N. Toosi University of technology, Tehran, Iran, in 1997, 2000, and 2005, respectively.

He is currently with Iran Telecommunication center Institute (ITRC), Tehran, Iran as the Chair of the Telecommunication and Cryptography Group.

Hojatolah Rohi received his B.Sc. degree in electronics and communication engineering from Amirkabir University of Technology (Tehran Polytechnic), Iran in 1993, and M.Sc., and Ph.D. Degrees in Electronics and Communication Engineering from K. N. Toosi University of technology, Tehran, Iran, in 1996 and 2005, respectively.

He is currently an assistant professor in Electrical Engineering department of the MUT University of Technology of Tehran at Iran.