2011

A Novel Channel Probing/Scanning Scheme for Secure Fast Handoff in IEEE 802.11-based Wireless Networks

Ye Yan
University of Nebraska-Lincoln, yy2318@ieee.org

Yi Qian
University of Nebraska-Lincoln, yqian2@unl.edu

Rose Qingyang Hu
Utah State University, rose.hu@usu.edu

This full text paper was peer reviewed at the direction of IEEE Communications Society subject matter experts for publication in the IEEE Globecom 2011 proceedings.

A Novel Channel Probing/Scanning Scheme for Secure Fast Handoff in IEEE 802.11-based Wireless Networks

Ye Yan, Yi Qian
Department of Computer and Electronics Engineering
University of Nebraska-Lincoln
Omaha, Nebraska 68182
Email: yy2318@ieee.org, yqian2@unl.edu

Rose Qingyang Hu
Department of Electrical and Computer Engineering
Utah State University
Logan, Utah 84322
Email: rose.hu@usu.edu

***Abstract*—With the proliferation of wireless networks for practical deployments in recent years, secure fast handoff has become significantly important to provide secured access while reduce the latency caused by handoff procedure. Channel probing/scanning delay has been a major contribution to the overall latency of handoff in IEEE 802.11 based wireless networks. In this paper, we present a novel secure fast handoff scheme that adopts network-assisted radio statement (NACS) to eliminate lengthy probing/scanning delay by taking advantage of the knowledge of network topology of neighboring nodes in the network. We apply an opportunistic mechanism to retrieve the channel condition from neighboring nodes close enough to reduce the scanning/probing delay while providing secure wireless access for the handoff candidate node. In this manner, it can reduce the channel probing/scanning delay and achieve secure handoff. We show analysis and simulation results to verify the performance of the proposed secure fast handoff scheme.**

I. Introduction

IEEE 802.11-based wireless networks have been widely accepted as a cost-effective technology for Internet access. However, fast handoff issue becomes a significant concern and ongoing effort when it comes to the stage of large scale commercial deployment. Since it has ignored the Layer 2 handoff in its early state, huge delay is introduced into handoff process by channel probeing/scanning operations like channel probe-response, multiple channel scan and SyncScan [1] etc. It severely undermines prior efforts towards fast handoff in IEEE 802.11 wireless networks. In this paper, we address the problems of existing IEEE 802.11 handoff probing/scanning mechanisms, by identifying the performance bottleneck and the possibility for improvement. Then, we propose a novel scheme for fast and secure handoff.

IEEE 802.11-based wireless networks consist of fixed access points (APs) and mobile clients (MCs). The APs connect to the backbone network via wired or wireless links. In early deployments of IEEE 802.11 based wireless networks, open access was a common practice which incurs the security concerns. Consequently, security measures are enforced which include basic WEP, WPA and WPA2. However, those security measures focus on authentication procedure which is right after channel probing/scanning. The previous probing/scanning procedures lack of security measures particularly.

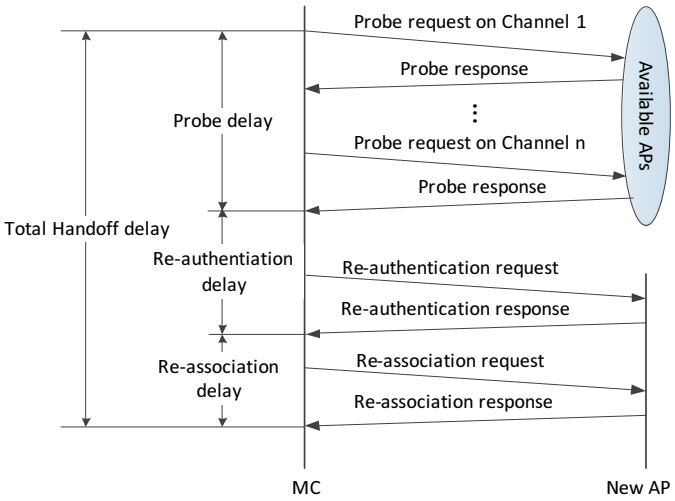

Fig. 1. Handoff Operations in IEEE 802.11 based Wireless Networks

The fundamental performance bottleneck of handoff in IEEE 802.11 wireless networks is caused by interruptions of data communications occurred in the event of MC changing its point of attachment, or AP. While the time-sensitive applications such as streaming media demands a delay of less than 300 ms and VoIP demands one less than 50 ms, as specified by International Telecommunication Union (ITU) standards [2], such tight latency requirements impose difficulties upon the primitive IEEE 802.11 network handoff mechanisms.

As illustrated in Figure 1, the handoff involves multiple dimensions of operations from the physical layer to the application layer. Conventionally, researches focused on Layer 2 and Layer 3 due to the fact that those contribute to the most of the overall handoff delay. Concerning Layer 3 handoff, it covers IP acquisition, route update, etc., and it has been well investigated. Mobile IP and its derivatives [3], [4] have been standardized as the major solutions. The situation about Layer 2 handoff is somewhat different and far from being mature. It involves operations including probing for candidate APs, mutual authentication between MC and AP, and association with target AP. The delay caused by authentication and association

978-1-4244-9268-8/11/$26.00 ©2011 IEEE

is determined by specific authentication mechanisms. It is obvious that various authentication methods, e.g. WEP/802.11X/, WPA/802.11i/WPA2, involve various ways of handshaking and exchanges of authentication signaling packets before data communications. The associated delay varies from several milliseconds to seconds. It is relatively fixed and simply similar to channel switch on Layer 1. However, on the contrary, there are different probing and authentication mechanisms existing in various implementations. Early research targets probing delay with assumption of open authentication which means no authentication at all; currently secured fast handoff tackles with probing delay with authentication enabled. The probing/scanning delay will accumulate to following authentication procedure. The longer probing/scanning procedure is, the less authentication latency quota left, since the total handoff latency is bounded in fast handoff. Therefore, the performance of secured handoff deteriorates.

In order to achieve secure and fast handoff performance in the real network operation environment, we propose an integrated solution, a novel Layer 2 fast handoff scheme - neighbor-assisted channel statement (NACS). The NACS scheme can eliminate the probing delay by taking advantage of the knowledge of neighboring MC, that is the channel condition of the neighboring MC which is close enough. We assume that MCs can overhear broadcasting of the neighboring APs and store the broadcasting as valid messages as long as the topology remains unchanged. In this sense, the delay caused by channel probing/scanning can be totally eliminated. Moreover, we also propose a key chain mechanism to counteract the security vulnerabilities to provide secured wireless access.

In the rest of this paper, we discuss the related work in Section II, and describe the proposed scheme in Section III. In Section IV we evaluate the performance of the proposed scheme. In Section V we give the conclusions.

II. Related Work

The fast handoff in IEEE 802.11 wireless networks involves three main operations: channel probing/scanning, authentication and association. In this section, we focus on channel probing/scanning operation and give a brief overview on the existing channel probing/scanning schemes for fast handoff. A quick summary on the corresponding advantages and disadvantages of the existing schemes is shown in Table I. Note that the term probing and scanning are interchangeable in the literature.

Since the channel probing delay is the main contribution to the overall handoff delay, many fast handoff schemes aim to reduce this lengthy process. Some schemes rely on reducing the number of scanning channels, the duration taken on each channel, scanning-related timers, etc. [5]. The tuning technique targets to find an optimal value for the time taken on each channel, i.e., MinChannelTime and MaxChannelTime to reduce active scanning delays [6]. Intelligent channel scanning aims to minimize the probing and waiting time on each channel [7]. SyncScan synchronizes MCs and APs and instructs MCs to scan the channels by switching channels at the exact moment when a beacon is about to arrive with periodic beacon broadcasting from APs [1]. Instead of probing all available channels individually, selective scanning reduces the number of channels required to discover APs. A number of selective scanning approaches have been proposed, such as selective scanning plus AP caching methods [8] designed to reduce Layer 2 handoff delay to a level where VoIP communication becomes seamless [7]. Another typical scheme is Neighbor Graph approach, which aim to reduce the total number of probed channels and the probe-waiting time on each channel via selective scanning as well as using caching techniques to solve the problem of packet loss [9]. MultiScan uses multiple radio interfaces equipped on MC to search proactively for alternate APs while being associated with an AP and interleaving data communications [10].

TABLE I
Comparison of fast channel probing/scanning mechanisms

	Features	Pros	Cons
Timer tuning	Optimize values of scanning timers	Simple and effective	Limited improvement
Intelligent channel scanning	Minimize the probing and waiting time on channels	Simple and effective	Limited improvement
SyncScan	Periodically probe channels in case of communication	Reduce the delay significantly	Large overhead
MultiScan	Use one radio to probe channels while another radio for communication	Minimize the delay to close to 0 ms	Extra hardware is required
Neighbor graph	Reduce the probed channels and probe-waiting time by using NG	Systematic enhancement of timer tuning and channel selection	Large overhead, limited improvement

III. Proposed Scheme

A. Motivation

There are certain factors behind the previous channel probing/scanning schemes. First, the design philosophy beneath all channel probing/scanning schemes is that the network topology always keeps changing, so that the topology information needs to be collected in a on-the-fly manner and keeps updating. Second, the schemes are mainly client-initiated, i.e., the handoff is employed at MC side rather than network side, which means the network information and intelligence have not been utilized during handoff.

Hence, we assume that the network topology is relatively static for APs, and the handoff decision can be made not only in a predetermined manner but also stand long. The delay caused by channel probing/scanning can be totally avoided and the collected topology information can be retrieved as long

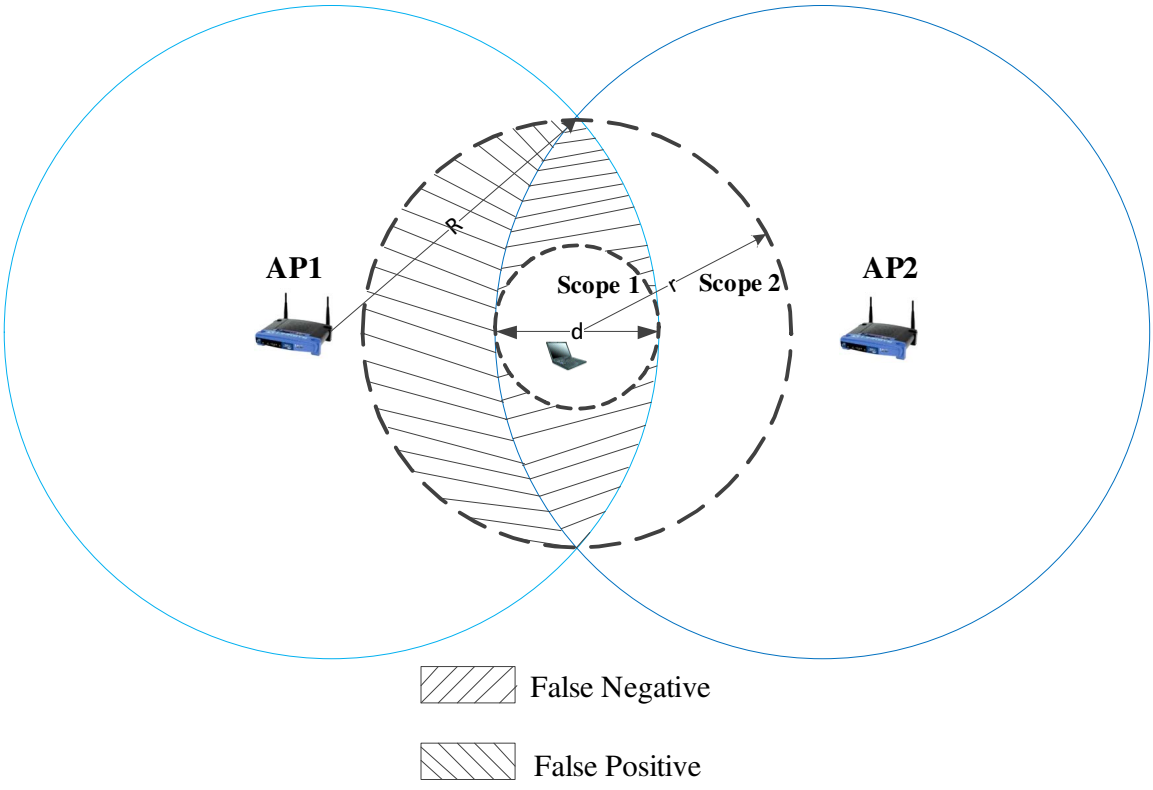

Fig. 3. Topology of NACS broadcasting

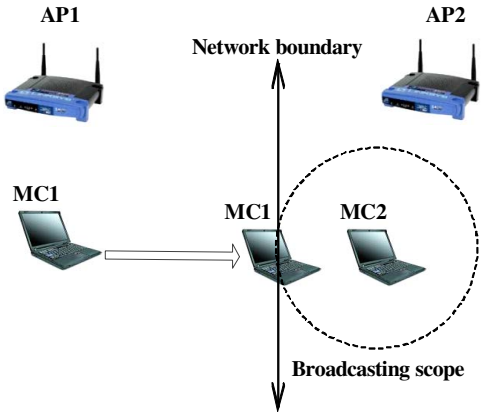

Fig. 2. Channel information provision from neighboring node broadcasting in NACS

as the neighboring APs remain active in the deployment. In order to proactively collect the network topology about APs, i.e. candidate APs for MC handoff, we introduce a training process into the operation in IEEE 802.11 based wireless networks. In order to comply with the de facto single radio MCs implementation, rather than those schemes with extra radios such as MultiScan [10], both APs and neighboring MCs have to coordinate to assist the handoff of MC. Based on the above discussions, we present the details of the proposed NACS scheme next.

B. System Overview

The fundamental design philosophy of the proposed NACS scheme is that the existing information of communication channels of neighboring MCs close enough to the candidate MC can help the handoff candidate MC to avoid the lengthy channel probing/scanning, and therefore eliminate most of the latency of handoff in IEEE 802.11 based wireless networks as illustrated in Fig. 2. It is necessarily to define the proper neighboring MCs broadcasting scope in handoff occasions to maintain the tradeoff between accuracy and efficiency.

As illustrated in Fig. 3, the smaller neighboring MC broadcasting scope (Scope 1) takes the advantage of accuracy whereas the larger neighboring MC broadcasting scope (Scope 2) covers entire intersection region of network coverage of adjacent AP1 and AP2. The entire Scope 1 is inside of the intersection region of network coverage of adjacent AP1 and AP2, whereas the complement region of Scope 1 within the intersection region of network coverage of adjacent AP1 and AP2 that cannot be covered by Scope 1 is defined as false negative. In the opposite, Scope 2 includes the whole intersection region of network coverage of adjacent AP1 and AP2 and plus other regions that may lead handoff candidate MC to wrong target AP or unnecessary handoff which is defined as false positive.

C. Key-Chain for Broadcast Message Authentication

Our proposed scheme employs an one-way hash chain [11] to secure the network protocol information. Key chains are

based on a hash function H with the property that its computation is easy, whereas its inverse H' is extremely difficult to compute. A hash chain with length n+1 is generated by applying H to an initial element (K_0) repeatedly for n times (i.e., $\forall 0 \leq i \leq n, K_{i+1} = H(K_i)$). AP periodically broadcast beacon message includes network topology information, message authentication code M(K_{i+1}), and previous message authentication key K_i. The beacon message of duration T_i is authenticated by message authentication function M($\cdot$) using the key K_{n+1-i}. The last value K_{n+1} after H has been applied n times is used as the first value of message authentication function M($\cdot$) in the broadcast message chain while the first value K_0 is unconcealed last as illustrated Fig. 4.

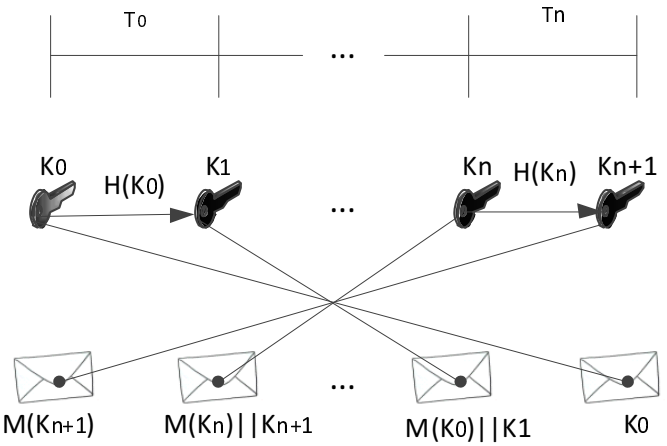

Fig. 4. One-way key chain and associated broadcast message authentication mechanism

With the AP's beacons broadcasted, the AP constructs hash chains continually. It generates consecutive one-way hash chains with length of n+1 starting from last value K_{n+1}.

D. NACS Handoff Procedure

As illustrated in Fig. 5, when an handoff candidate MC moves into the intersection region of two or more adjacent APs' coverage areas, the handoff candidate MC finds the radio signal degrades below certain predefined radio signal criteria. Then, MC send a NACS_HO_Request to its associated AP to initiate the NASC handoff procedure. After received the NACS_HO_Request from MC, AP sends NACS_HO_Response with message authentication key K_{n+1} to MC and broadcast the handoff candidate MC's NACS_Request with message authentication code $M(n)$ in all potential channels using its preferred channel list which is maintained by the AP.

The radio channel characteristics between associated AP and MC are monitored by each MC. For instance, one on-the-fly measurement, the Received Signal Strength Indicator (RSSI), is recoded by MC during each transmission and overhearing. It constitutes the radio channel statement in the neighbor-assist handoff scene. The neighboring APs and the corresponding radio channel is updated in AP's database after a successful handoff. Thus the database is looked up to find the most recent updated channel stored for next handoff. According to the update, a most recent handoff neighboring AP, is also the most potential AP the next MC handoff to associate with. After the successful NACS, the fast handoff is initiated and managed by the network side rather than MC only. In this manner, channel probing/scanning delay is totally eliminated since the MC does not probe for candidate APs in all channels anymore when handoff occurs.

After neighboring MC hears the NACS_Request with message authentication code $M(n)$ from AP, it can authenticate immediately the received broadcasting message to see if it is validated or not since it keeps on overhear the AP's beacon broadcasting before. If the received NACS_Request is validated, refer to previous beacon broadcasting and unconcealed broadcast message authentication keys. The neighboring MC broadcast NACS_Response and message authentication code using K_{n+1}, is the previous unconcealed message authentication key. The neighboring MC controls its broadcasting scope with the certain radius to obtain the tradeoff between accuracy and efficiency which is specified in NACS_Request.

Only those handoff candidate MC within the broadcasting scope can receive and authenticate the NACS_Request as the genuine one from the neighboring MC which is close enough as a reliable reference to the current and nearby channel condition. After authenticated the received NACS_Response, handoff candidate MC sends AP a NACS_HO_Acknowledgement to finalize its NACS handoff as well as the target AP channel condition from neighboring MC's NACS_Response. After received the NACS_HO_Acknowledgement, AP can release the association with the handoff candidate MC and update the neighboring network topology information such as the neighboring APs and the corresponding radio channel in its database as mentioned above.

In case of no NACS_Response or invalidated NACS_Response received during whole NACS duration, the handoff candidate MC will perform the legacy channel probing/scanning, as in the traditional handoff procedure.

IV. Performance Evaluation

A. False Analysis

In this section, we assume the MCs to be uniformly distributed and mobilized. Given any mobile MC in the intersection region of two or more adjacent AP network coverage areas but not in the broadcasting region, the Scope 1 as shown in Fig. 3, are suffered the false negative effect. So, the false negative rate of neighboring MC broadcasting can be calculated as

$$\begin{aligned} Rate_{FalseNegative} &= \frac{Area(Flase\text{Negative})}{Area(Intersection)} \\ &= \frac{S_R - S_r - S_{RA}}{S_R} \end{aligned} \tag{1}$$

where

$$S_R = \frac{\arcsin(\frac{\sqrt{R^2-(R-\frac{d}{2})^2}}{R})R^2 - \sqrt{R^2-(R-\frac{d}{2})^2}(R-\frac{d}{2})}{2} \tag{2}$$

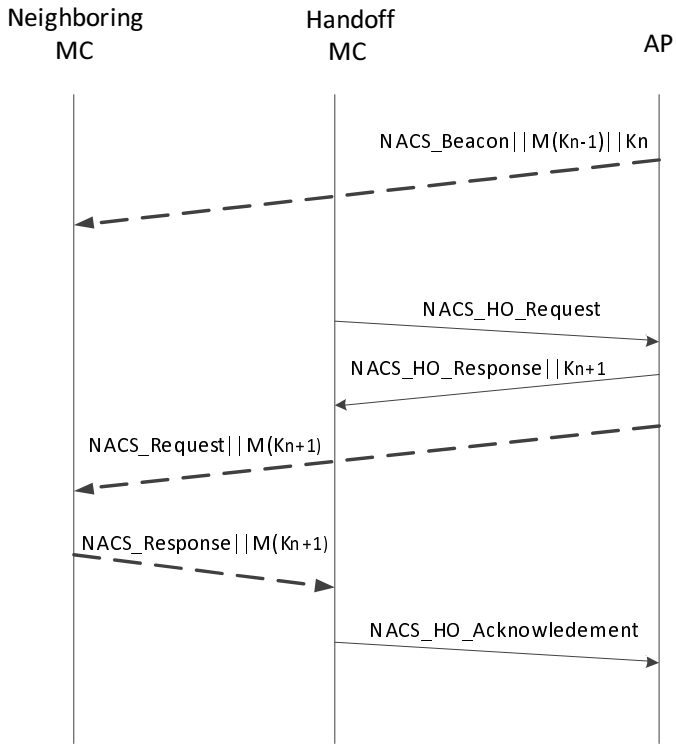

Fig. 5. NASC Handoff Procedure

$$S_r = \frac{[\frac{\pi}{2} - \arcsin(\frac{2 \cdot SA}{R - d/2}) - \arcsin(\frac{2 \cdot SA}{R})]r^2}{2} \quad (3)$$

$$S_{RA} = \frac{\arcsin(\frac{2 \cdot SA}{R - d/2})R^2}{2} - SA \quad (4)$$

and

$$SA = \sqrt{p(p-R)(p-r)[p-(R-\frac{d}{2})]} \quad (5)$$
$$p = \frac{R + r + (R - \frac{d}{2})}{2}$$

If a neighboring MC broadcasts its NACS_Response packet to a larger area, say Scope 2 as shown in Fig. 3, to enlarge the efficiency of NACS handoff, it will have to compromise the accuracy, namely cause the false positive effect.

Again, we assume that the MC are uniformly distributed and mobilized. The estimated false positive rate of neighboring MC broadcasting is

$$Rate_{FalsePositive} = \frac{Area(Flase\text{Positive})}{Area(Scope)} = \frac{2(\frac{S_O}{4} - S_{RA} - S_r)}{S_O} \quad (6)$$

where

$$S_O = \pi r^2 \quad (7)$$

We can get the above relationship of false area from the basic relative neighboring MC broadcast and network topology parameters such as the neighboring MC broadcasting radius r, AP coverage radius R and the width of intersection of adjacent APs' coverage. From those parameters, we can estimate the false rate and find the optimal system parameter setting to maintain the tradeoff of accuracy and efficiency as discussed in following.

B. Numerical Results

Fig. 6 to Fig. 9 illustrate the results given by Equ. 1 and Equ. 6, with the width of intersection of adjacent APs' coverage d is 2 and 4 meters and network coverage radius R is 50 and 100 meters respectively. From those figures, we can observe that the greater the neighboring MC broadcast radius r is, the larger false positive rate is while less the false negative rate is for handoff candidate MC performing the proposed NACS handoff scheme. Since the neighboring MC broadcast radius r is a controllable parameter, we can set the proper neighboring MC broadcast radius r to maintain the tradeoff between false positive rate and false negative rate, namely system accuracy and efficiency. The meeting point of the curves of false positive rate and false negative rate, could be an example of the proper balance point for both false positive and false negative effect in the proposed NACS handoff.

On the other hand, the width of intersection of adjacent APs' coverage d and network coverage radius R are uncontrollable system parameters, they affects greatly our proposed NACS handoff scheme in both false positive rate and false negative rate as well as the meeting point of the curves as the possible system balance point.

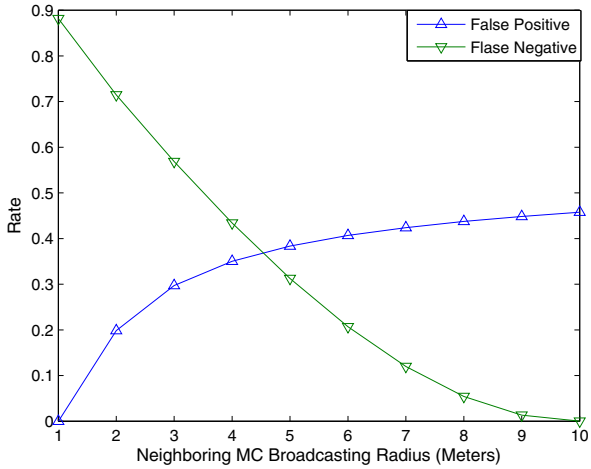

Fig. 6. False negative rate vs. false positive rate in different neighboring MC broadcast coverage with Network Intersection Width d=2 Meters and network coverage radius R=50 meters

V. Conclusion

In this paper, we proposed a secure and fast handoff scheme to facilitate handoff procedure in IEEE 802.11 based wireless networks by using one-way hash chain and retrieving neighboring node's channel condition record and network topology information. Instead of lengthy channel probing/scanning

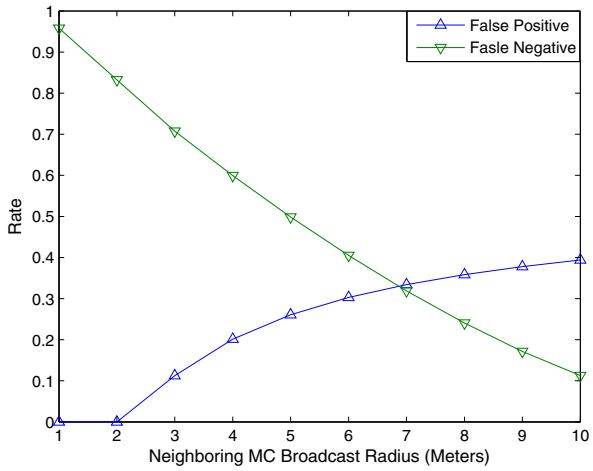

Fig. 7. False negative rate vs. false positive rate in different neighboring MC broadcast coverage with Network Intersection Width d=4 Meters and network coverage radius R=50 meters

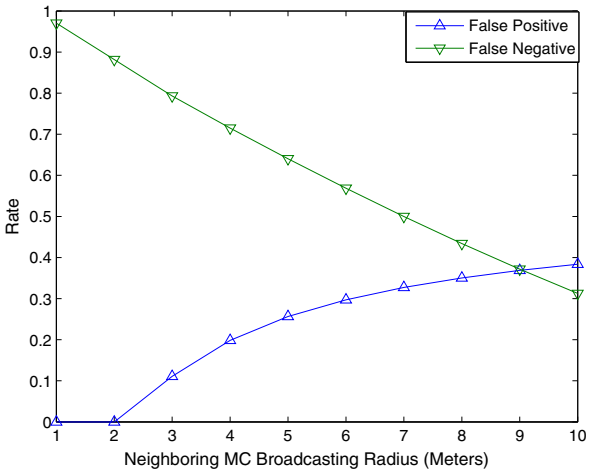

Fig. 9. False negative rate vs. false positive rate in different neighboring MC broadcast coverage with Network Intersection Width d=4 Meters and network coverage radius R=100 meters

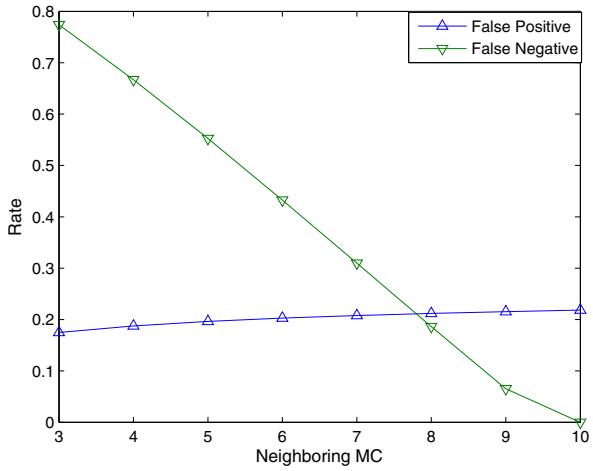

Fig. 8. False negative rate vs. false positive rate in different neighboring MC broadcast coverage with Network Intersection Width d=2 Meters and network coverage radius R=100 meters

process used in legacy handoff procedures, we retrieve channel condition record and network topology information from neighboring nodes of the neighbor node within certain distance to maintain the tradeoff of accuracy and efficiency. We further propose using an one-way hash chain for broadcast message authentication function key generation and distribution to avoid possible attacks an adversary could mount on legacy channel probing/scanning related broadcast messages, and provided simple and effective counter measures against them. Finally, we provided a comprehensive performance evaluation of our proposed scheme in term of false positive rate and false negative rate. We also tested our scheme with different system parameters such as various width of intersection of adjacent APs' coverage and neighboring MC broadcast radius. Our future work will include performance evaluation in practical physical radio signal coverage using our proposed scheme, and also the optimal secure fast handoff design.

REFERENCES

[1] I. Ramani and S. Savage, "SyncScan: practical fast handoff for 802.11 infrastructure networks," Proc. of IEEE INFOCOM 2005, pp. 675-684 vol. 1, 2005.

[2] CCITT, 1988, International Telecommunication Union, General Characteristics of International Telephone Connections and International Telephone Circuits.

[3] D. Johnson, C. Perkins and J. Arkko, "Mobility support in IPv6", IETF RFC3775, June 2004.

[4] R. Ramjee, K. Varadhan, L. Salgarelli, S. R. Thuel, S.-Y. Wang, T. La Porta, "HAWAII: A domain-based approach for supporting mobility in wide-area wireless networks," IEEE/ACM Transactions on Network,Volume:10, issue 3, pp.396-410, June 2002.

[5] A. Mishra, M. Shin and W. Arbaugh, "An empirical analysis of the IEEE 802.11 MAC layer handoff process," ACM SIGCOMM Computer Communications Review, vol. 33, no. 2, pp. 93-102, Apr. 2003.

[6] H. Velayos and G. Karlsson, "Techniques to reduce the IEEE 802.11b handoff time," Proc. of IEEE ICC 2004, Paris, France, pp. 3844-3848, June 20-24, 2004.

[7] K. Kwon and C. Lee, "A fast handoff algorithm using intelligent channel scan for IEEE 802.11 WLANs," Proc. of the ICACT 2004, Phoenix Park, Republic of Korea, pp. 46-50, Feb. 9-11, 2004.

[8] S. Pack, J. Choi, T. Kwon and Y. Choi,"Fast-handoff support in IEEE 802.11 wireless networks," IEEE Communications Surveys & Tutorials, vol. 9, no. 1, pp. 2-12, Jan. 2007.

[9] S. Shin, A. G. Forte, A. S. Rawat and H. Schelzrinne, "Reducing MAC layer handoff latency in IEEE 802.11 wireless LANs," Proc. of ACM MobiWac04, Philadelphia, PA, USA, pp. 19- 26, Oct. 1, 2004.

[10] V. Brik, A. Mishra, and S. Banerjee, "Eliminating Handoff Latencies in 802.11 WLANs using Multiple Radios: Applications, Experience, and Evaluation," Proc. ACM Internet Measurement Conf. 2005, Oct. 2005.

[11] L. Lamport, "Password Authentication with Insecure Communication," Comm. ACM, vol. 24, no. 11, pp. 770-772, Nov. 1981.