Control Channel Jamming Mitigation under Node Capture Attacks

B.Thenral[1], B. Bakkiaya Lakshmi[2], K. S. Shanthamathi[3]
[1, 2, 3] Department of ECE
[1, 2, 3] Ganadipathy Tulsi's Jain Engineering College, Vellore, Tamilnadu, India

Abstract- *Availability of service in many wireless networks depends on the ability for network users to establish and maintain communication channels using control messages from base stations and other users. The use of spread spectrum techniques can deter an external adversary from such control channel jamming attacks. However, malicious colluding insiders or an adversary who captures or compromises system users is not deterred by spread spectrum, as they know the required spreading sequences. For the case of internal adversaries, we propose a framework for control channel access schemes using the random assignment of cryptographic keys to hide the location of control channels. We propose and evaluate metrics to quantify the probabilistic availability of service under control channel jamming by malicious or compromised users and show that the availability of service degrades gracefully as the number of colluding insiders or compromised users increases. We propose an algorithm called GUIDE for the identification of compromised users in the system based on the set of control channels that are jammed. We evaluate the estimation error using the GUIDE algorithm in terms of the false alarm and miss rates in the identification problem.*

Keywords- Wireless multiple access, control channel jamming, security, node capture attacks, probabilistic metrics.

I. INTRODUCTION

Efficient communication in mobile networks requires the use of multiple access protocols allowing mobile users to share the wireless medium by separating user data in any combination of time, frequency, signal space, and physical space. The entire class of multiple access can thus be described by the unifying framework of orthogonal frequency division multiple access (OFDMA). Allocation of access and resources to mobile users must be periodically updated in order to maintain the efficiency of the multiple access protocol when base station group membership, user demands, and wireless channel conditions are dynamic. Hence, there is a necessary overhead involved in the multiple access protocol to handle the resource allocation to users. This overhead often takes the form of control messages exchanged between mobile users and base stations. In many systems, dedicated channels are established for the exchange of control messages. These control channels can be used for a wide variety of functions, from topological information propagation for network routing to access control in subscription services. In a cellular system such as GSM [3], [4], [5], for example, base stations and mobile users must coordinate over a variety of control channels in order to perform access control, traffic channel allocation, and intercell user handoff. Control channels thus serve as a platform on which higher-level protocol functionality is supported and, hence, as critical points of failure that can be targeted by a malicious adversary in a denial-of-service. We thus approach the problem of designing control channel access schemes which allow for efficient reception of control messages while maintaining a degree of independence between the hopping sequences held by different users. In this work, we focus our attention on designing schemes which are robust to control channel jamming attacks by malicious colluding insiders or compromised users.

A. Problem Statement and Contributions:

In this paper, we develop a framework for control channel access schemes that are robust to control channel jamming. Furthermore, we provide techniques for random allocation of control channels to users which yield graceful performance degradation as the number of compromised users increases. Our contributions are summarized as follows:

We develop a correspondence between the problems of key establishment and control channel access in wireless networks and develop a framework for control channel access schemes providing probabilistic availability of control messages using random key assignment. We propose metrics of resilience and delay to quantify the probabilistic availability of service and the quality of provided service, respectively, under control channel jamming attacks. We evaluate the proposed metrics by extending existing results for resilience to node capture in wireless networks. We propose techniques for the identification and revocation of compromised users by the service provider or a trusted authority that need not be constantly online. We formulate the identification problem as a maximum likelihood estimation problem and provide greedy heuristic algorithms using information available to the service

provider. We evaluate the identification algorithm by approximating the false alarm and miss rates under the greedy algorithms. We provide a simulation study to demonstrate trade-offs that exist between robustness to control channel jamming and resource expenditure which result from the use of random key assignment protocols, serving as a foundation for the design.

II. MODEL ASSUMPTIONS

We state the assumed models for the multiple access protocol and control message structure, adversary, and service provider or trusted authority. We provide a summary of the notation used throughout this work in Table.

TABLE 1
A Summary of Notation is Provided

Symbol	Definition
$\mathcal{U}, B$	Set of U users, B base stations
p	Number of time slots in the reuse period
$\mathcal{K}_t$	Set of channel identifiers, or keys, for time slot t
q_t	Number of control channels in time slot t, $\lvert\mathcal{K}_t\rvert$
$\mathcal{K}_{tu}$	Subset of $\mathcal{K}_t$ assigned to user u
m_t	Number of keys per user in time slot t, $\lvert\mathcal{K}_{tu}\rvert$
$\mathcal{C}, c$	Set and number of compromised users, $c = \lvert\mathcal{C}\rvert$
$\mathcal{K}_{t\mathcal{C}}$	Subset of $\mathcal{K}_t$ held by $\mathcal{C}$
$\mathcal{J}_t$	Subset of $\mathcal{K}_{t\mathcal{C}}$ corresponding to jammed channels
θ_t	Probability that each key $k \in \mathcal{K}_{t\mathcal{C}}$ is added to $\mathcal{J}_t$
$r_t(c)$	Slot resilience for time slot t
$r(c)$	Resilience to control channel jamming
$d_t(c)$	Initial-slot delay for time slot t
$d(c)$	Delay due to control channel jamming
$\widehat{\mathcal{C}}$	Estimate of set $\mathcal{C}$ of compromised users
$\mathcal{F}(c)$	False alarm rate in the estimate $\widehat{\mathcal{C}}$ of $\mathcal{C}$
$\mathcal{M}(c)$	Miss rate in the estimate $\widehat{\mathcal{C}}$ of $\mathcal{C}$

Control Message Access Model:

We describe the multiple access protocol in terms of the OFDMA with separation of signals over orthogonal carrier signals and in time as follows. We denote the set of M orthogonal carriers used for wireless communication. We assume that time is slotted and that an initial portion of each time slot is dedicated to control messages. Since we are focusing on the availability of control messages in this paper, we ignore the portion of each time slot dedicated to data. We further partition each time slot t into S subslots with duration sufficient to transmit a single control message.

RANDOM KEY ASSIGNMENT FRAMEWORK FOR CONTROL CHANNEL ACCESS:

In this section, we develop a correspondence between the problems of control channel access and symmetric key assignment. We show that efficient and robust control channel access can be provided using random key assignment, yielding a framework for probabilistic control channel access schemes.

Problem Mapping:

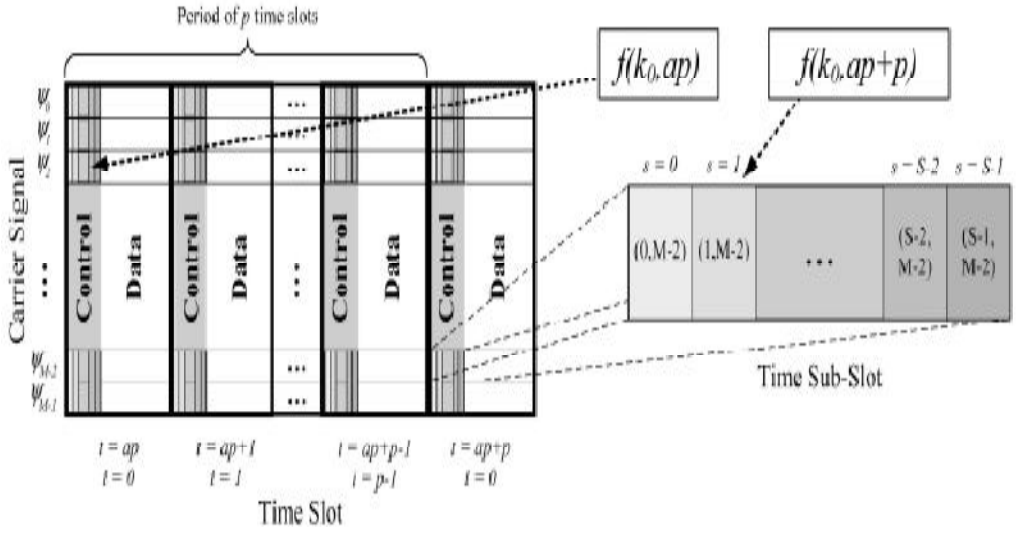
We provide a one-to-one mapping between control channel access for multiple users in a single time slot and the assignment of symmetric keys to network nodes for use in cryptographic protocols. The mapping is formalized by constructing a bipartite graph which uniquely maps between control channel access schemes and symmetric key assignment schemes.

Random Assignment of Control Channel Keys

we make use of the symmetric key assignment model in to provide a framework for probabilistic control channel access using random key assignment. The proposed framework can then be used to design control channel access schemes which are robust to jamming by compromised users. For the remainder of this paper, we use the term control channel key interchangeably with control channel identifier.

AVAILABILITY OF CONTROL MESSAGES UNDER CONTROL CHANNEL JAMMING:

In order to evaluate the effect of control channel jamming by compromised users, we define and evaluate metrics to quantify the probabilistic availability of control messages. We note that users in the proposed control channel access scheme as outlined do not exchange any information about the assigned keys Kiu, so the adversary cannot obtain any deterministic information about the key assignment.



IDENTIFICATION OF COMPROMISED USERS:

In this section, we formulate a statistical estimation problem for the identification of compromised users by the TA, constructing a setbC of suspected jammers to eliminate from the network with no knowledge of the number of compromised users. Due to the complexity of the resulting identification problem, we propose two algorithms, collectively referred to as GUIDE (Greedy User Identification), based on a greedy heuristic which ranks users according to the likelihood of being a compromised
user. Finally, we approximate the estimation error resulting from the GUIDE algorithms.

GUIDE-Θ: Greedy Estimate of $\mathcal{C}$
Given: $\mathcal{J}, \Theta$

$\hat{\mathcal{C}} \leftarrow \emptyset$
while $\mathcal{J} \not\subseteq \mathcal{K}_{\hat{\mathcal{C}}}$ **do**
  $u^* \leftarrow \arg\max_{u \in \mathcal{U} \setminus \hat{\mathcal{C}}} \Gamma(u|\mathcal{J}, \Theta)$
  $\hat{\mathcal{C}} \leftarrow \hat{\mathcal{C}} \cup \{u^*\}$
end while

Fig. 3. The algorithm GUIDE-Θ constructs a greedy estimate $\hat{\mathcal{C}}$ of the set $\mathcal{C}$ of compromised users using the jamming evidence $\mathcal{J}$ and parameter Θ.

Greedy Identification of Jammer Known Instead of basing the identification of jammers on the probability over subsets of U, we base the identification on the probability that a user is a compromised user. This heuristic reduces the set estimation problem to a set membership estimation problem. We refer to the identification algorithm as GUIDE, for the Greedy User Identification algorithm, and first address the case when is known to the TA. In this case, the TA uses a greedy algorithm to construct by adding users in decreasing order of probability until satisfies the condition.This GUIDE-_ lgorithm is given in Fig. 3. We note that ties can be roken arbitrarily in the arg max function, though it is also ossible that the arg max function can choose an entire ubset of users to add to bC This technique and its implications are not addressed in this paper.

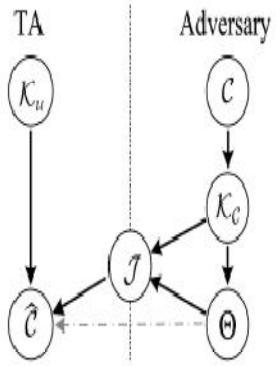


Fig. 2. The information available to the TA and the adversary during the attack and identification process is illustrated. The TA has knowledge of the parameters $\mathcal{K}_u$ and $\mathcal{J}$ and uses this available information to construct an estimate $\hat{\mathcal{C}}$ of $\mathcal{C}$. The adversary has knowledge of the parameters $\mathcal{C}, \mathcal{K}_{\mathcal{C}}, \Theta$, and $\mathcal{J}$. The dotted line from Θ to $\hat{\mathcal{C}}$ indicates that the TA may or may not know Θ.

III. NUMERICAL ILLUSTRATION AND DESIGN

In this section, we provide simulation results to illustrate design trade-offs, providing a basis for parameter

selection in design of the system simulate the long-term performance of the system as a function of the identification interval of the TA as defined .

Simulation Setup:

We simulate a network of users with varying parameter values of p, mi, and qi with the jamming probability. For each set of parameters p, mi, and qi, we randomly assign p sets of mi control channel keys to each user from the p sets of qi keys. For each value of c, the subset C is randomly selected from the set of users U and the subsets J i of keys used for jamming are selected randomly using the parameter _i. For each subset C of size c, the resilience is computed as the fraction of the remaining users that can access at least one control channel. Similarly, the average delay , false alarm rate, and miss rate are computed using the GUIDE algorithm based on the assigned keys, jammed control channels, and compromised users. Each data point in our simulation reflects an average over 100 simulated network and random key assignment instances. The solid and dashed lines in each plot represent the analytical results derived in and the symbol-marked points represent the results of the simulation study. As can be seen from Fig. 5, the analytical results for the resilience and the average delay coincide. While the analytical and simulation results for the false alarm rate and the miss rate disagree at individual values of c, the analytical results provide a reasonable approximation of the error behavior that can be expected.

Trade-Offs in Key Assignment Parameters:

We next identify and discuss design trade-offs in key assignment parameters by investigating the impact of individual parameters using the proposed evaluation metrics. We compare resource trade-offs with respect to the required key storage mi for users in U and qi for base stations in B.We note that since each key corresponds to a unique control channel, the communication overhead for base stations is proportional to the base station key storage.

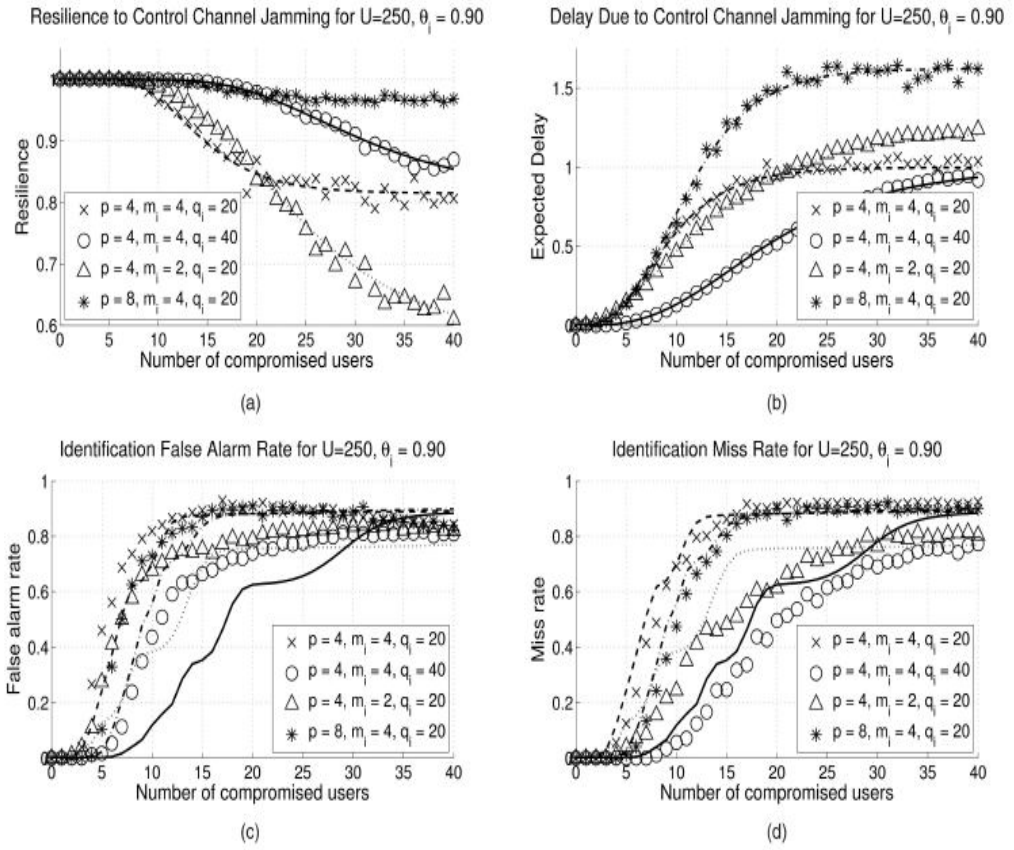


Fig. 5. Variations in the (a) resilience $r(c)$, (b) expected delay $\bar{d}(c)$, (c) false alarm rate $\mathcal{F}(c)$, and (d) miss rate $\mathcal{M}(c)$ are illustrated for a network of $U = 250$ users with varying parameter values of p, m_i, and q_i and a jamming parameter of $\theta_i = 0.9$ using GUIDE-Θ. Solid and dashed lines represent analytical results derived in Sections 4 and 5, and symbol-marked points represent the simulated results averaged over 100 simulated network instances.

IV. CONCLUSION

In this paper, we addressed the mitigation of control channel jamming by malicious colluding insiders and compromised system users as well as the identification of compromised users without prior knowledge of the number of compromised users in the system. We mapped the problem of control channel access that is robust to jamming by compromised users to the problem of secure key establishment under node capture attacks. Based on the mapping, we proposed a framework for control channel access schemes using random key assignment. We proposed and evaluated metrics for resilience and delay which quantify the availability of control messages under control channel jamming attacks, and demonstrated that the use of random key assignment provides graceful degradation in availability as the number of compromised users increases. We formulated the identification of compromised users in the system as a maximum likelihood estimation problem and proposed the GUIDE algorithms using greedy heuristics for jammer identification.

REFERENCES

[1] Patrick Tague, Mingyan Li, and Radha Poovendran,"Mitigation of Control Channel Jamming under Node Capture Attacks", IEEE TRANSACTIONS ON MOBILE COMPUTING, VOL. 8, NO. 9, SEPTEMBER 2009

[2] P. Tague, M. Li, and R. Poovendran, "Probabilistic Mitigation of Control Channel Jamming via Random Key Distribution," Proc. 18th Ann. IEEE Int'l Symp. Personal, Indoor, and Mobile Radio Comm. (PIMRC '07), Sept. 2007.

[3] K. Fazel and S. Kaiser, Multi-Carrier and Spread Spectrum Systems. Wiley, 2003.

[4] T.S. Rappaport, Wireless Communications: Principles and Practice, second ed. Prentice Hall, 2001.

[5] J. Schiller, Mobile Communications. Addison-Wesley, 2000.

[6] G.L. Stu¨ ber, Principles of Mobile Communications, second ed. Kluwer, 2001.

[7] R. Anderson, Security Engineering: A Guide to Building Dependable Distributed Systems. John Wiley & Sons, Inc., 2001.

[8] A. Chan, X. Liu, G. Noubir, and B. Thapa, "Control Channel Jamming: Resilience and Identification of Traitors," Proc. IEEE Int'l Symp. Information Theory (ISIT '07), June 2007.

[9] A. Perrig, J. Stankovic, and D. Wagner, "Security in Wireless Sensor Networks," Comm. ACM, vol. 47, no. 6, pp. 53-57, June 2004.

[10] W. Xu, W. Trappe, and Y. Zhang, "Channel Surfing: Defending Wireless Sensor Networks from Interference," Proc. Sixth Int'l Conf. Information Processing in Sensor Networks (IPSN '07), pp. 499-508, Apr. 2007.

[11] M. ^Cagalj, S. ^Capkun, and J.-P. Hubaux, "Wormhole-Based Antijamming Techniques in Sensor Networks," IEEE Trans. Mobile Computing, vol. 6, no. 1, pp. 100-114, Jan. 2007.

[12] L. Eschenauer and V.D. Gligor, "A Key-Management Scheme for Distributed Sensor Networks," Proc. Ninth ACM Conf. Computer and Communications Security (CCS '02), pp. 41-47, Nov. 2002.

[13] B. Parno, A. Perrig, and V. Gligor, "Distributed Detection of Node Replication Attacks in Sensor Networks," Proc. IEEE Symp. Security and Privacy, pp. 49-63, May 2005.

[14] P. Erdo¨ s, P. Frankl, and Z. Fu¨ redi, "Families of Finite Sets in Which No Set is Covered by the Union of r Others," Israel J. Math., vol. 51, nos. 1/2, pp. 79-89, 1985.

[15] D.J.C. MacKay, Information Theory, Inference, and Learning Algorithms. Cambridge Univ. Press, 2003.