The 18th Annual IEEE International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC'07)

PROBABILISTIC MITIGATION OF CONTROL CHANNEL JAMMING VIA RANDOM KEY DISTRIBUTION

Patrick Tague*, Mingyan Li*†, and Radha Poovendran*
*Network Security Lab (NSL), Department of Electrical Engineering, University of Washington, Seattle, Washington
†Boeing Phantom Works, Seattle, Washington
Email: {tague, myli, rp3}@u.washington.edu

ABSTRACT

The use of distinct, dedicated communication channels to transmit data and control traffic introduces a single point of failure for a denial of service attack, in that an adversary may be able to jam control channel traffic and prevent relevant data traffic. Hence, it is of interest to design control channel access schemes which are resilient to jamming. We map the problem of providing resilient control channel access under jamming to that of secure communication channel establishment. We propose the use of random key distribution to hide the location of control channels in time and/or frequency. We evaluate performance metrics of resilience to control channel jamming, identification of compromised users, and delay due to jamming as a function of the number of compromised users.

I. INTRODUCTION

To provide service to users in a wireless network, communication channels must be established for user data as well as network and application control data. Control channels can be used for a wide variety of services, from propagation of network topology for routing, to access control in subscription services. In a cellular system [1,2], for example, base stations coordinate with system users over a variety of control channels in order to perform access control, traffic channel allocation, station-to-station handoff, and a number of other functions.

In many wireless networks, the control data serves as the platform on which higher protocol data is transported and user service is provided. Without access to control packets, users in an application setting will be unable to establish connections with servers and, thus, be unable to receive service. Hence, control channels serve as a single point of failure that can be targeted by a malicious adversary. In particular, an adversary can perform a denial-of-service (DoS) attack [3,4] by jamming the system's control channels.

The authors of [5] showed that precise knowledge of the frequency band and time interval of each control channel allows an adversary to jam only the control channels and reduce the required power by several orders of magnitude compared to jamming the entire system. The use of cryptographic primitives was then proposed in [5] to hide the location of control channels in time and/or frequency. The proposed approach made use of keyed hash functions to locate the control channels such that any user with a valid key can locally compute a control channel location. By assuming that no more than a fixed maximum number of colluding or compromised users exist in the system, the authors developed key distribution schemes based on error-correcting codes [6] and Sperner Theory [7]. The advantage of the scheme in [5] is that as long as the number of compromised users is below the threshold, every valid user is guaranteed to locate a control channel that is not jammed, and every colluder can be detected and eliminated. However, the scheme's strength also leads to many disadvantages. First, the maximum number of compromised users must be known *a priori*. Second, if the number of compromised users exceeds the threshold by even one, the entire system can degenerate with no guarantees of control packet reception or detection of colluders. More importantly, given that adversary models for wireless networks are not well known and are yet emerging [8], it is not realistic to assume a constant maximum number of users will be compromised. In the absence of well-defined adversary models, it is of interest to *develop a framework with graceful performance degradation* as the number of compromised users increases.

In this work, we propose the use of random key distribution for resilience to control channel jamming and statistically characterize the performance as a function of the number of colluding or compromised users. We make use of results for secure communication in [9,10] in developing key distribution and analyzing system performance. This approach allows the system designer to choose the degree of probabilistic resilience to collusion or user compromise without fixing a threshold number of colluding or compromised users *a priori*. The absence of such a threshold introduces a high degree of flexibility into the design. This allows the system designer to analyze the average or worst-case system performance due to compromise of users. The result is smooth performance degradation as a function of the number of compromised users.

The remainder of this paper is organized as follows. Control channel access and adversary assumptions are outlined in Section II. In Section III, we map the problem of resilient control channel access to the establishment of secure communication channels and provide a framework for resilient control channel access schemes via random key distribution. Metrics for performance of key distribution schemes under control channel jamming are evaluated in Section IV. Implementation trade-offs between efficiency and resilience are discussed in Section V. Section VI summarizes our contributions and comments on future work.

II. PRELIMINARIES

We state our assumptions about the control channel access model for users in the wireless network. In addition, we state our assumptions about the goals and capabilities of the adversary.

1-4244-1144-0/07/$25.00

A. Control Channel Access Model

The network consists of N mobile wireless users and a collection of base stations or servers. Mobile users receive control packets from the servers using a set of control channels which are distributed over both time and frequency. Time is assumed to be slotted into a set of p time slots which are repeated periodically such that at time n, users access control channels within slot $i \equiv n \pmod{p}$. Each control channel is arbitrarily located in time and frequency and that the time duration of a control packet is negligible compared to that of a time slot.

Servers transmit a common control packet over all control channels in a period of p time slots. To enable control channel hiding, both system and user are required to locate control channels within a time slot using a *control channel locator function* $f(k_{i\ell}, n)$, where $k_{i\ell}$ is a *control channel identifier* that uniquely identifies the ℓ^{th} control channel in time slot i and n is the current time such that $i \equiv n \pmod{p}$. The control channel access model is illustrated in Fig. 1.

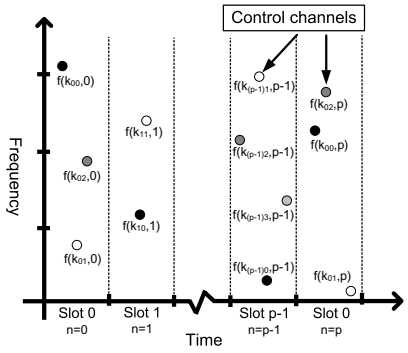

Figure 1: Control packets are sent over redundant channels arbitrarily located in time and frequency within each slot. Users and system servers locate control channels using a function f and control channel identifiers $k_{i\ell}$ for slot i.

B. Adversary Model

A group of malicious users under such a control channel access model may be able to locate a significant portion of control channels. The malicious users can then collude to jam the accessible control channels and deny service to honest users. Alternatively, an external adversary can compromise valid users and assume their identities in the network. A single adversary then acts as a group of malicious colluders to jam the accessible control channels similar to the case above. As the effect of internal and external adversaries on the control channel access scheme are indistinguishable, they are combined into a common adversary model.

Users that are either malicious insiders or those that have been compromised by an external adversary are hereafter referred to as *compromised users*, and the set of such users is denoted $\mathcal{C}$. We assume that the adversary will jam every control channel that can be located using the keys held by compromised users.

III. Resilience to Control Channel Jamming

The ability for a set of compromised users to locate and jam a set of control channels depends on the control channel locator function f outlined in Section II-A. The question of particular interest is how to provide user access to control channels via f while maintaining a degree of resilience to jamming by compromised users. In this section, we map resilient control channel access to the well-studied problem of establishing secure communication in wireless networks.[1]

A. Problem Mapping

We provide a mapping between the problem of resilient control channel access and the problem of establishing secure communication channels in wireless networks. For the remainder of this work, we assume that the p time slots in each period are independent and, thus, outline the mapping for a single time slot.

The desired mapping is constructed in the form of a bipartite graph [11] with left and right node sets respectively corresponding to the set of users and the set of control channels. An edge between a left and a right node exists whenever the corresponding user has the required control channel identifier $k_{i\ell}$ to compute the control channel location $f(k_{i\ell}, n)$. Hence, the channel can be jammed as soon as the adversary compromises a user with $k_{i\ell}$, represented as a symmetric cryptographic key [12]. Two left nodes joined to a common right node correspond to a pair of users that share a symmetric key, thus indicating that the users can establish a secure communication channel. An adversary compromises the security of an established channel as soon as one user with the corresponding key $k_{i\ell}$ is compromised.

The above mapping between control channel access and secure communication establishment allows the key distribution framework in [9] to be applicable to the setting of resilient control channel access. In particular, the control channel locator function can be implemented using a keyed cryptographic hash function [12] as in [5], and a compromised user with a *control channel key* $k_{i\ell}$ can jam any locatable control channels. Metrics of resilience to control channel jamming can thus be defined as a function of the key distribution scheme used to allocate control channel keys to users.

B. Random Control Channel Key Distribution

In what follows, we describe *random control channel key distribution* using the framework of [9]. Table 1 summarizes the notation used throughout this work.

Let $\mathcal{K}_i = \{k_{i0}, \ldots, k_{i(q_i-1)}\}$ denote the set of q_i control channel keys used to locate the q_i control channels in slot i. The sets $\mathcal{K}_i$ are assumed to be pairwise disjoint. Each user $j \in \{0, \ldots, N-1\}$ is assigned a subset $S_{ij} \subseteq \mathcal{K}_i$ of m_i control channel keys for each slot i denoted $S_{ij} = \{s_{ij}^{(0)}, \ldots, s_{ij}^{(m_i-1)}\}$.[2] Using the key distribution framework in [9], the subsets S_{ij} for each slot i can be randomly selected from $\mathcal{K}_i$ while probabilistically controlling the number $\lambda(k_{i\ell})$ of subsets containing each key $k_{i\ell}$. The variables $\lambda(k_{i\ell})$ are controlled by specifying the probability distribution $\mathcal{P}_i(\lambda)$ of

[1] The reader is referred to [9] for an extensive list of references.

[2] It is not essential that m_i is the same for each user. This extension is described and analyzed in [10].

the variables as a parameter to the key distribution algorithm. The only constraint on the validity of a distribution $\mathcal{P}_i$ is that it yields an average $\mu_i = Nm_i/q_i$.

The above setup thus provides a framework for random control channel key distribution. In what follows, we evaluate probabilistic performance metrics with respect to the given framework. The analytical results can then be used to design a key distribution scheme for a particular application or setting.

Table 1: A summary of notation is provided for reference.

Symbol	Definition
N	number of users
p	number of time slots
q_i	number of channels in slot i
$\mathcal{K}_i$	set of channel keys for slot i
m_i	number of keys in $\mathcal{K}_i$ per user
S_{ij}	set of $\mathcal{K}_i$ assigned to user j
$\lambda(k_{i\ell})$	number of users with $k_{i\ell} \in S_{ij}$
$\mathcal{P}_i(\lambda)$	probability distribution of $\lambda(k_{i\ell})$
μ_i	average of $\mathcal{P}_i(\lambda)$, equal to $\frac{Nm_i}{q_i}$
$\mathcal{C}$	set of compromised users
$r_j(c)$	resilience of j to c compromised users
$r(c)$	average resilience over all users
$\rho_j(c)$	probability j is falsely accused for $\lvert\mathcal{C}\rvert = c$
$\rho(c)$	average of $\rho_j(c)$ over all j
$d(c)$	delay due to jamming for $\lvert\mathcal{C}\rvert = c$

IV. Performance Analysis

The performance of random control channel key distribution schemes in the framework of Section III-B is evaluated with respect to the set of compromised users $\mathcal{C}$. We focus on the average performance as a function of the number of compromised users $c = |\mathcal{C}|$, noting that the worst-case performance probabilities can be derived using [10].

A. Resilience to Compromised Users

The performance of a random control channel key distribution scheme can be evaluated in terms of the ability for a given user to access a control channel that can not be jammed by compromised users. The probabilistic metric of *resilience to compromised users* is thus defined as follows.

Define $r_j^i(c)$ as the probability that user j can access a control channel in time slot i that is not jammed by the c compromised users. This is equivalent to the probability that user j has a control channel key in $\mathcal{K}_i$ that is not held by any of the c compromised users, given by

$$r_j^i(c) = \Pr\left[S_{ij} \not\subseteq \bigcup_{t\in\mathcal{C}} S_{it}\right] = 1 - \Pr\left[S_{ij} \subseteq \bigcup_{t\in\mathcal{C}} S_{it}\right]. \quad (1)$$

The resilience for user j is then defined as the probability $r_j(c)$ that user j can access at least one control channel in the p slots that can not be jammed by the c compromised users, given by

$$r_j(c) = 1 - \prod_{i=0}^{p-1} \left(1 - r_j^i(c)\right). \quad (2)$$

The resilience can further be averaged over all users $j \in \{0, \ldots, N-1\}$ and expressed as $r(c)$. The intermediate step of computing $r_j^i(c)$ is provided by Lemma 1.

Lemma 1. *The probability $r_j^i(c)$ can be approximated as*

$$r_j^i(c) \approx 1 - \prod_{m=0}^{m_i-1} \left(1 - \left(\frac{N - \lambda\left(s_{ij}^{(m)}\right)}{N-1}\right)^c\right).$$

Proof. The probability $r_j^i(c)$ given in (1) can be written as

$$r_j^i(c) = 1 - \prod_{m=0}^{m_i-1} \left(1 - \Pr\left[s_{ij}^{(m)} \notin S_{it}, t \in \mathcal{C}\right]\right) \quad (3)$$

$$\approx 1 - \prod_{m=0}^{m_i-1} \left(1 - \prod_{t\in\mathcal{C}} \Pr\left[s_{ij}^{(m)} \notin S_{it}\right]\right). \quad (4)$$

Since there are exactly $\lambda\left(s_{ij}^{(m)}\right)$ users that hold the key $s_{ij}^{(m)}$, the probability that a compromised user does not hold $s_{ij}^{(m)}$ is

$$\Pr\left[s_{ij}^{(m)} \notin S_{it}\right] = \frac{N - \lambda\left(s_{ij}^{(m)}\right)}{N-1}, \quad (5)$$

and substitution of (5) into (4) completes the proof.[3] □

The resilience $r_j(c)$ for user j can then be computed using (2) and the result of Lemma 1. The average resilience for any user in the system can then be computed using Theorem 2 as follows.

Theorem 2. *The average resilience $r(c)$ for $c = |\mathcal{C}|$ compromised users can be approximated as*

$$r(c) \approx 1 - \prod_{i=0}^{p-1} \left(1 - \left(\frac{N-\mu_i}{N-1}\right)^c\right)^{m_i},$$

where μ_i is the expected value of $\lambda(s_{ij}^{(m)})$ according to a probability distribution $\mathcal{P}_i(\lambda)$.

Proof. The result is obtained from (2) and Lemma 1 by replacing each $\lambda(s_{ij}^{(m)})$ with its expected value μ_i. □

When $q_i = q$ and $m_i = m$ for all i, the resilience $r(c)$ in Theorem 2 takes the form

$$r(c) \approx 1 - \left(1 - \left(\frac{N-\mu}{N-1}\right)^c\right)^{mp}. \quad (6)$$

The above analysis yields the average resilience probability taken over all sets of compromised users $\mathcal{C}$ such that $|\mathcal{C}| = c$ and does not assume that the adversary has any knowledge about the keys assigned to each user. If the adversary is able to identify the set of keys assigned to each user, the worst-case resilience probability can be derived using the attack framework provided in [10].

[3] An alternate proof can be derived by mapping the resilience of the control channel key distribution scheme to a key distribution scheme known as the Q-composite scheme [13] and applying the analysis of [9].

B. Identification of Compromised Users

A desirable property of a resilient control channel access scheme is the ability for servers to identify the set of compromised users in a centralized manner. Assuming the server maintains a record of the sets S_{ij} and can detect jamming, it may be possible to identify the set of compromised users, revoke them from the system, and update the remaining users with fresh keys. However, if all of the keys held by a valid user are held by compromised users, the valid user may be *falsely accused* and revoked from the system, characterized probabilistically as follows.

Let $\rho_j(c)$ be the probability that user j is falsely accused by the centralized server when there are c compromised users. Given that the adversary jams all accessible control channels, the probability of false accusation is exactly the complement of the resilience probability $r_j(c)$ for user j. Hence, the probability $\rho_j(c)$ can be approximated using the results of Lemma 1 and Theorem 2. When $q_i = q$ and $m_i = m$ for all i, the false accusation probability $\rho(c)$ can be approximated using Theorem 2 as

$$\rho(c) \approx \left(1 - \left(\frac{N-\mu}{N-1}\right)^c\right)^{mp}. \tag{7}$$

Given the probabilities $r(c)$ and $\rho(c) = 1-r(c)$, the probability distribution of the number $M(c)$ of falsely accused users can be computed as a function of the number of compromised users c as follows.

Theorem 3. *The probability that $M(c) = \eta$ of the $(N-c)$ valid users are falsely accused when there are c compromised users is approximated as*

$$\Pr[M(c) = \eta] \approx \binom{N-c}{\eta} \rho(c)^\eta r(c)^{N-c-\eta}.$$

Proof. This result follows by treating each false accusation as a Bernoulli random variable with probability $\rho(c) = 1 - r(c)$, yielding the desired binomial representation. □

The result of Theorem 3 can be used to evaluate further metrics of false accusation such as the expected number of falsely accused users, given by the mean of the distribution, or the probability that the c compromised users are uniquely identified, given by $\Pr[M(c) = 0]$.

C. Delay

When there are compromised users in the system and a fraction of control channels are jammed, a user may have to wait for multiple time slots before an accessible channel is available. We are thus interested in the distribution of user delay as a function of the number of compromised users c.

With probability $1 - r_j(c)$, every control channel that can be located by user j is jammed, and j will never be able to access a control channel, corresponding to an infinite delay. However, with probability $r_j(c)$, user j will have a finite delay of 0 to $(p-1)$ time slots. We thus compute the conditional delay of user j given that the delay is finite. Suppose that a user $j \notin \mathcal{C}$ attempts to access a control channel at time n and the next accessible control channel is not available to user j until time n', $n \le n' \le n+p-1$. The delay for user j at time n is thus defined as $d_j(c,n) = n' - n$.[4] The distribution of this user delay is characterized as follows.

Lemma 4. *The probability distribution $\Pr[d_j(c,n) = \delta]$ of delay for user j is given by*

$$\Pr[d_j(c,n) = \delta] = \gamma r_j^{n+\delta \bmod p}(c) \prod_{d=0}^{\delta-1} \left(1 - r_j^{n+d \bmod p}(c)\right)$$

where γ is a normalization constant to ensure the probability sums to 1 over all $\delta \in \{0, \ldots, p-1\}$.

Proof. The probability that user j must wait δ time steps before a channel is available is exactly the probability that there is no channel available at times $n, \ldots, n+\delta-1$ and there is a channel available at time $n+\delta$. For each n', the probability that there is not a channel available is $\left(1 - r_j^{n' \bmod p}(c)\right)$, and the probability that there is a channel available is $r_j^{n' \bmod p}(c)$. □

When $q_i = q$ and $m_i = m$ for all i, the slot-specific resilience probabilities $r_j^i(c)$ for all i will be equal and the delay distribution will not depend on n on average. The delay can further be averaged over all users $j \notin \mathcal{C}$ as $d(c)$ as follows.

Theorem 5. *The average delay $d(c)$ when $q_i = q$ and $m_i = m$ satisfies the probability distribution*

$$\Pr[d(c) = \delta] = \frac{r^0(c)}{r(c)} \left(1 - r^0(c)\right)^\delta$$

where $r^0(c)$ is the slot-specific resilience for each of the p time slots obtained by averaging $r_j^0(c)$ over all users j.

Proof. Since $q_i = q$ and $m_i = m$, the slot-specific resilience $r_j^i(c)$ is equal for all i and can be replaced in the result of Lemma 4 by $r_j^0(c)$. Averaging over all users $j \notin \mathcal{C}$ effectively replaces each $r_j^0(c)$ with $r^0(c)$. The normalization constant $\gamma = 1/r(c)$ is computed algebraically using the fact that the summation of $\Pr[d(c) = \delta]$ is a finite geometric sum. □

The results of Lemma 4 and Theorem 5 characterizing user delay can then be used to study delay characteristics. For example, the expected value of the delay distribution yields the expected average delay $D(c)$ of users in the system as a function of the number of compromised users c and is illustrated in Fig. 2.

V. Discussion

The framework in Section III-B and the performance analysis in Section IV can be used to design control channel key distribution schemes with a variety of application- and platform-specific details. Unlike a deterministic scheme [5], there is little dependence between the parameters p, q_i, and $m_i \le q_i$ in a

[4] Note that n and n' may exist in adjacent *periods* of the control channel access scheme, corresponding to reception of distinct control packets. In most applications this corresponds to the user obtaining a fresh control packet and, thus, is not an issue. In special cases, missing a control packet may have a more serious impact, but we do not address this issue.

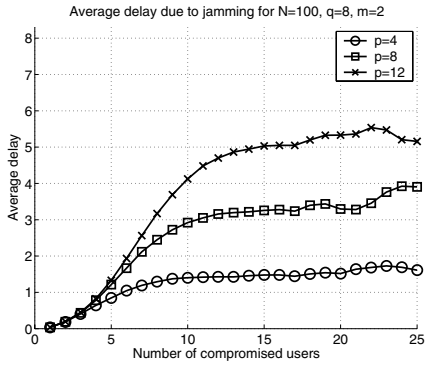

Figure 2: The average delay as a function of the number of compromised users c is simulated for $N = 100$ users with $m_i = m = 2$ keys each out of $q_i = q = 8$ total keys per slot. The number of slots p is varied to illustrate delay dependence on p.

random scheme. However, various trade-offs can be identified between the protocol efficiency or overhead and the resilience to compromised users. Due to space limitation, we identify these trade-offs and leave the detailed analysis for future work.

A. Varied Number of Slots

As seen in Lemma 1 and Theorem 2, an increase in the number of time slots p will lead to an exponential improvement in the resilience to attack. However, this leads to a linear increase in key storage for each user and system server. In addition, if there are a large number of compromised users, the average delay between receiving successive control packets increases linearly with p, as can be seen in Fig. 2.

B. Varied Number of Keys

The resilience probability given in Theorem 2 and the definition $\mu_i = Nm_i/q_i$ suggest that increasing both m_i and q_i by a constant multiple a does not change μ_i, yielding an exponential improvement in resilience to compromised users. Hence, a linear increase in both user and server storage leads to an exponential improvement in resilience. This also increases the total number of control channels and, thus, increases the system overhead. The trade-off between storage and resilience is illustrated in Fig. 3.

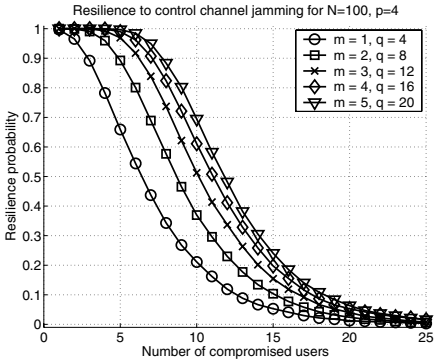

Figure 3: The resilience probability $r(c)$ in (6) is evaluated via simulation for $N = 100$ users in a system with $p = 4$ time slots. The values $m_i = m$ and $q_i = q$ are scaled such that m/q is constant, illustrating the improvement in resilience $r(c)$ as key storage increases.

VI. Conclusion

In this work, we showed that the problem of resilient control channel access under jamming can be mapped to the problem of establishing secure communication channels. In order to ensure graceful performance degradation, we proposed the use of random key distribution for resilience to control channel jamming. We evaluated the performance metrics of resilience to compromised users, identification of compromised users, and delay due to jamming as a function of the number of compromised users. We also discussed various trade-offs between resilience and resource efficiency that arise from the flexibility resulting from random key distribution. Our future work will consider an intelligent adversary making use of selective jamming to avoid identification and revocation from the system.

Acknowledgments

This work is supported in part by the following grants: ONR YIP, N00014-04-1-0479; ARO PECASE, W911NF-05-1-0491; NSA/DoD IASP Fellowship; and ARL CTA.[5]

References

[1] T. S. Rappaport. *Wireless Communications: Principles and Practice*. Prentice Hall, 2nd edition, 2001.

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

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

[4] M. Li, I. Koutsopoulos, and R. Poovendran. Optimal jamming attacks and network defense policies in wireless sensor networks. In *Proc. 26th IEEE International Conference on Computer Communications (INFOCOM'07)*, pages 1307–1315, Anchorage, AK, USA, May 2007.

[5] A. Chan, X. Liu, G. Noubir, and B. Thapa. Control channel jamming: Resilience and identification of traitors. In *Proc. IEEE International Symposium on Information Theory (ISIT'07)*, Nice, France, June 2007.

[6] R. M. Roth. *Introduction to Coding Theory*. Cambridge University Press, 2006.

[7] K. Engel. *Sperner Theory*. Cambridge University Press, 1997.

[8] B. Parno, A. Perrig, and V. Gligor. Distributed detection of node replication attacks in sensor networks. In *Proc. 2005 IEEE Symposium on Security and Privacy*, pages 49–63, Oakland, CA, USA, May 2005.

[9] P. Tague and R. Poovendran. A canonical seed assignment model for key predistribution in wireless sensor networks. *ACM Transactions on Sensor Networks*, 2007, to appear.

[10] P. Tague and R. Poovendran. Modeling adaptive node capture attacks in multi-hop wireless networks. *Ad Hoc Networks*, 5(6):801–814, August 2007.

[11] R. Diestel. *Graph Theory*. Springer, 3rd edition, 2005.

[12] A. J. Menezes, P. C. van Oorschot, and S. A. Vanstone. *Handbook of Applied Cryptography*. CRC, 1996.

[13] H. Chan, A. Perrig, and D. Song. Random key predistribution schemes for sensor networks. In *Proc. 2003 IEEE Symposium on Security and Privacy*, pages 197–213, Oakland, CA, USA, May 2003.

[5]This document was prepared through collaborative participation in the Communications and Networks Consortium sponsored by the U. S. Army Research Laboratory under the Collaborative Technology Alliance Program, DAAD19-01-2-0011. The U. S. Government is authorized to reproduce and distribute reprints for Government purposes notwithstanding any copyright notation thereon. The views and conclusions contained in this document are those of the author and should not be interpreted as representing the official policies, either expressed or implied, of the Army Research Laboratory or the U. S. Government.