Connectivity in Wireless Networks with Dynamic Key Compromise and Recovery

Satashu Goel Aylin Yener
Wireless Communications and Networking Laboratory
Electrical Engineering Department
The Pennsylvania State University, University Park, PA 16802
goel@psu.edu yener@engr.psu.edu

***Abstract*—This paper considers the problem of key management in wireless networks. In particular, we investigate the effect of dynamic key compromise and recovery on connectivity in large networks. A queuing model with a finite buffer is used to model the dynamics of key compromise. The exact distribution of the fraction of keys compromised is obtained. The result of the queuing analysis is used to determine the probability of outage, where an outage occurs whenever instantaneous end-to-end connectivity, in percolation sense, is not present. Numerical results show that in order to obtain a low outage probability, it is critical that key compromises are detected accurately, and that the average key recovery rate has a weak influence on the outage probability. Thus, for the same average key recovery rate the system must be designed to have a high key recovery probability rather than a large number of key recoveries per unit time with a low key recovery probability.**

I. Introduction

Wireless ad-hoc networks will undoubtedly have wide usage in the near future due to their extensive range of potential applications [1]. However, the broadcast nature of the wireless medium makes it easy to eavesdrop upon ongoing communications. Providing information security in wireless ad-hoc networks poses a considerable challenge because computationally expensive cryptographic schemes, such as public key cryptography, may not be practical due to limited processing capabilities of the communication nodes. Private or symmetric key cryptography may be used, however, the distribution of keys is a challenge, because it may not be possible to predetermine the neighborhood of each node, especially if the nodes are mobile.

A significant research effort has been directed towards the design and analysis of key distribution schemes for symmetric key cryptography [2], [3], [4], and detection and revocation of compromised keys [5]. Several key distribution schemes have been proposed which aim to minimize the memory and communication requirements of communication nodes while ensuring that each link is secured with high probability. Although the problems of key management have been studied extensively for *static* networks, the dynamics of the key compromise and recovery has received limited attention.

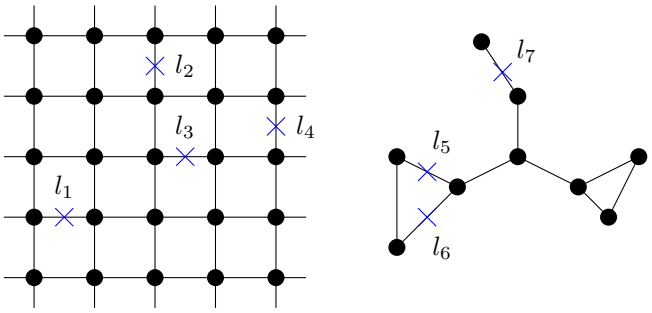
In this paper, we model the scenario where new link compromises occur at each time-instant due to repeated attacks on the network. Some of the compromised nodes may be recovered through periodic network maintenance. The recovery occurs with probability p_{rec}, which is the probability that the link compromises are known and the network maintainer is available. We present a simple queuing model with finite buffers to model time-varying key compromises. In this setup, the queue *stores* compromised keys, which are *serviced* when they are recovered. The effect of the number of key compromises on end-to-end connectivity is captured by the percolation threshold, which specifies the maximum fraction of keys compromised such that connectivity is present in the network, with high probability. The queuing model is used to obtain the exact stationary distribution of the fraction of links compromised. Using this distribution, we obtain the outage probability where an outage occurs whenever end-to-end connectivity is not present. We observe from the numerical results that it is critical to detect key compromises with a high probability, in order to obtain a low outage probability. In particular, the average rate of key recovery can be misleading and has a weak influence on the outage probability.

In related work, percolation theory has been used to study connectivity in the context of information theoretic secrecy, in [6], where the concept of secrecy graph was introduced. Connectivity with uncertain location of eavesdroppers and correlated failures was considered in [7]. The impact of key compromise on connectivity when keys are randomly predistributed, was considered in [8]. However, a static network was considered, while this paper considers time-varying key compromises. Connectivity in networks with time-varying links has been considered in [9], though not in the context of security. Epidemic theory has been used to model the spread of node compromises, perhaps through a virus or worm, in wireless networks [10]. Although this model captures the dynamics of the spread of node compromise, starting from a single point of failure, it does not model the process of repeated compromise and recovery.

It is worth reiterating that the goal of this work is to provide a framework that captures both the time-varying security failures and the geometry of the network, and characterize the connectivity properties. This is accomplished by combining ideas from queuing and percolation theories.

The remainder of the paper is organized as follows. In Section II, the queuing model for dynamic key compromise and recovery is presented, and the outage probability is defined. In Section III, the exact stationary distribution of the fraction of keys compromised is obtained. Numerical results are presented

978-1-4244-8015-9/10/$26.00 ©2010 IEEE



(a) (b)

Fig. 1. (a) Failures in square lattice (b) Failures in a random graph

in Section IV. Section V concludes the paper.

II. Model and Formulation

Let $\hat{G} = (\phi, \hat{E})$ denote a geometric graph in $\mathbb{R}^d$, where $\phi = \{x_i\} \subset \mathbb{R}^d$ is the set of locations of legitimate nodes. Let $\delta(x, y) = \|x - y\|$ denote a distance metric, which is assumed to be Euclidean distance in this paper. $\hat{E}$ is the set of links in the graph. The links in $\hat{E}$ are determined using the Gilbert disk graph model, i.e., the link $(x, y) \in \hat{E}$ if $\delta(x, y) \leq r$, where the distance threshold r ensures a minimum signal to noise ratio at the receiver. Thus, $\hat{E}$ is the set of links over which reliable communication is possible. Graph $\hat{G}$ can be a lattice graph, where the legitimate nodes are located on the vertices of a lattice, and each node is connected to its nearest neighbors. An example is a square lattice in $\mathbb{Z}^2$ with the distance threshold of 1. Fig. 1 shows a square lattice where links l_1, l_2, l_3 and l_4 have been compromised, and a random graph where links l_5, l_6 and l_7 have been compromised.

A secrecy graph $G = (\phi, E)$ is defined based on the underlying geometric graph $\hat{G}$, such that each link in the secrecy graph is both reliable and secure. The secrecy graph was defined in [6] in the context of information theoretic secrecy, where link security is provided using channel coding. In this paper, security of a link is ensured using private key cryptography. Link (x, y) is secure if the nodes located at x and y share a private key. We assume a secret key distribution mechanism so that each link is secured using a separate cryptographic key. An example of such a scheme is a random key pre-distribution scheme [2], [3], where each node is assigned K cryptographic keys at random out of a pool of N keys. Then, the probability that two nodes share at least one cryptographic key is

$$p_{key} = 1 - \frac{\binom{N-K}{K}}{\binom{N}{K}} \tag{1}$$

if $K \leq N/2$ and $p_{key} = 1$ otherwise. It is assumed that if two nodes share a key through the key pre-distribution scheme, they set up a *unique* key to secure the link for future use. Hence, all links in the secrecy graph have unique private keys associated with them. For simplicity, we will assume that $K > N/2$, so that $p_{key} = 1$, throughout the analysis. We will observe later in the paper that, if $K \leq N/2$, the effect of $p_{key} < 1$ can be incorporated into the analysis.

We will focus on the key compromises in secrecy graph $G = (\phi, E)$. We assume that the adversary can overhear communication between nodes and perform cryptanalysis to identify the secret keys. Further, we assume that an intrusion detection scheme exists, e.g. in [11], which identifies the compromised keys.

A. Dynamic key compromise and recovery

We consider a network $G^{(L)} = (\phi^{(L)}, E^{(L)})$ with L links. Key compromise and recovery are assumed to occur at discrete time instants. At time k, adversaries are able to compromise $A_k^{(L)}$ links in the network, where the compromised keys are chosen independently. The model is valid, for example, when the network is localized and the adversary can listen to communication over all the links, and hence, compromise links at random through cryptanalysis. In Section III-B, we will discuss a model with correlated failures, which is similar to the model considered in [7]. A static scenario was considered in [7], whereas this paper considers time-varying failures and recoveries.

At time $k = mT$, the network maintainer can recover a maximum of $B_{mT}^{(L)}$ compromised links, where T is a positive integer and $m \in \mathbb{N}$. The underlying assumption is that the link compromises can be detected reliably so that key recovery is possible. The uncertainty in key recovery is modeled by assuming a distribution on $B_{mT}^{(L)}$. We assume that no links are recovered at other time instants, i.e., $B_{mT+l} \doteq 0$ if $0 < l < T$. $\{A_k^{(L)}\}$ and $\{B_{mT}^{(L)}\}$ are assumed to be i.i.d. and independent of each other. Their distributions are assumed to be known to the system designer.

An example of this model would be a wireless network which is maintained at a specific time each day. Every hour, certain number of the links may be compromised due to attacks by adversaries. Then, $T = 24$, $\{A_k^{(L)}\}$ would represent the number of links compromised per hour and $\{B_{mT}^{(L)}\}$ would represent the number of links that are recovered per day. The number of compromised links at time k is denoted by $C_k^{(L)}$. $C_k^{(L)}$ is given by the recursive equation

$$C_k^{(L)} = \min(L, (C_{k-1}^{(L)} + A_k^{(L)} - B_k^{(L)})^+) \tag{2}$$

where $(x)^+ \doteq \max(0, x)$. The minimum in (2) is due to the fact that the number of compromised links cannot exceed L. Note that the (2) is similar to the update equation for a queuing system. Notice that here we consider a sequence of graphs $G_k^{(L)} = (\phi^{(L)}, E_k^{(L)})$, where $E_k^{(L)}$ is the set of non-compromised links at time k.

B. Percolation Threshold and Outage Probability

The concept of percolation was introduced by Broadbent and Hammersley [12], to model the diffusion process in materials. They modeled porosity of materials using regular lattices, where each node is present with a certain probability to indicate whether the flow of liquid is blocked or not.

We consider a bond percolation problem where each link is present with probability p. Percolation is said to occur if an infinite connected component exists in the corresponding graph. It was shown that a phase transition exists, i.e., there exists a critical threshold, below which all components are finite almost surely, and above which an infinite component exists almost surely. Let us denote the number of nodes in the component containing the origin by N_0. Then, the percolation probability is defined as

$$\theta(p) = P(N_0 = \infty). \tag{3}$$

The percolation threshold is defined as [13]

$$p_c = \sup\{p : \theta(p) = 0\}. \tag{4}$$

Roughly, p_c is the largest value of p for which an infinite component does not exist in the lattice. In other words, for any $p > p_c$, the lattice will have an infinite component containing the origin, almost surely. Percolation threshold exists for geometric graphs and secrecy graphs as well.

Note that the percolation threshold is defined in (4) for a static network. However, in the previous section, we described a dynamic scenario where connectivity in the graph is time-varying. In order to capture the dynamics of connectivity, we define an outage event. An outage is declared at time k if the graph does not have end-to-end connectivity, in the sense of percolation. For a large network ($L \to \infty$), let the fraction of keys compromised, in the steady state ($k \to \infty$), be denoted by C, assuming that a stationary distribution exists. Then, an outage occurs whenever $1 - C < p_c$, where p_c is the percolation threshold for a given geometric graph. Therefore,

$$P_{outage} = \Pr\{C > 1 - p_c\}. \tag{5}$$

Notice that the distribution of C depends on the queuing process, while the percolation threshold depends on the geometry of the network, and the assumptions on key compromise and recovery processes, e.g., whether they are i.i.d. or correlated. Here, the assumption is that node compromise and recovery occur at a much slower time scale compared to the time scale over which routing algorithms converge after change in network topology. Thus, (5) is the probability that *instantaneous* connectivity is not present in the secrecy graph.

Note that the model presented in this paper holds for any geometric graph, and the outage probability can be obtained whenever percolation threshold is known. In particular, percolation thresholds are known for triangular and square lattices, and outage probabilities for these lattices are obtained in Section IV.

III. Connectivity with dynamic key compromise and recovery

In this section, we present an exact solution for the stationary distribution of the fraction of keys compromised in the limit $L \to \infty$, assuming that the key compromise and recovery processes scale with L. We note that the appropriate scaling along with the inherent discrete nature of the problem allows for the exact solution. The outage probability defined in (5) can be obtained using the stationary distribution.

A. Stationary distribution of the fraction of key compromises

We consider a sequence of graphs $G^{(L)} = (\phi^{(L)}, E^{(L)})$, indexed by the number of links $L \in L_0\mathbb{Z}^+$, where L_0 is a positive integer. It is assumed that the number of key compromises and recoveries scale with L,

$$A_k^{(L)} = LA_k \tag{6}$$

$$B_k^{(L)} = LB_k \tag{7}$$

for some $\{A_k\}$ and $\{B_k\}$ and $L \in L_0\mathbb{Z}^+$. A_k is the fraction of links compromised at time k, and it has a distribution f_A. B_k is the fraction of links recovered at time k, and it has a distribution f_B when $k = mT$. B_k is identically zero when $k \neq mT$. Since we have assumed that $A_k^{(L)}$ and $B_k^{(L)}$ scale linearly with L, the fraction of keys compromised at time k is obtained as $\tilde{C}_k \doteq \tilde{C}_k^{(L)} = C_k^{(L)}/L$.

We focus on the time instants $k = mT$, where $m \in \mathbb{N}$. Define $D_m \doteq \sum_{i=0}^{T-1} A_{mT-i} - B_{mT}$ and $C_m \doteq \tilde{C}_{mT}$. f_D denotes the distribution of D_m. Then, the dynamics at $k = mT$ is given by,

$$C_m = \min(1, (C_{m-1} + D_m)^+). \tag{8}$$

Let us assume that a stationary distribution exists for $\{C_m\}$ and let the corresponding random variable be denoted by C.

The stationary distribution of $\{C_m\}$ can be obtained using the standard technique of spectral factorization [14], which does not assume a finite buffer, corresponding to a finite network. Notice that the equation in (8) is linear if $0 \leq C_{m-1} + D_m \leq 1$. Then the distribution of C can be written as

$$f_C(c) = \begin{cases} (f_C * f_D)(c), 0 \leq c \leq 1 \\ 0, \text{ otherwise} \end{cases} \tag{9}$$

The main difficulty here is that (9) is non-linear. It can be made linear by introducing an auxiliary variable C^- with distribution f_{C^-} so that,

$$f_C(c) + f_{C^-}(c) = (f_C * f_D)(c). \tag{10}$$

Taking the z-transform of both sides, and re-arranging the terms, we obtain

$$\frac{\Phi^-(z)}{\Phi(z)} = D(z) - 1. \tag{11}$$

The transforms $\Phi^-(z)$ and $\Phi(z)$ can be obtained by spectral factorization of $D(z) - 1$ [14], and $\Phi(z)$ can be inverted to obtain the steady state distribution of C. The limitation of this approach is that depending on the discretization, one may have to factorize a high degree polynomial and invert a complicated rational function. We now present a solution based on a system of linear equations, which overcomes this limitation, and is simpler and more intuitive. This method is valid as long as the assumption of linear scaling on $A_k^{(L)}$ and $B_k^{(L)}$ holds. Numerical results in the next section are obtained using this method.

Notice that $\tilde{C}_k^{(L)}$ takes discrete values and the same discretization can be used for all $L \in L_0\mathbb{Z}^+$ due to the linear

scaling of $A_k^{(L)}$ and $B_k^{(L)}$. In particular, for $L = L_0$, the range of $\tilde{C}_k^{(L_0)}$ consists of $(L_0 + 1)$ values in the set

$$\{0, 1/L_0, 2/L_0, \ldots, 1\} \tag{12}$$

Let the probability mass function (p.m.f.) of C is denoted by $\mathbf{p} \doteq (p_0, p_1, \ldots, p_{L_0+1})$. Then, the stationary distribution, if it exists, must satisfy,

$$p_0 = \sum_{j=0}^{L_0+1} p_j (\sum_{k \leq 0} f_D(-j+k)) \tag{13}$$

$$p_n = \sum_{j=0}^{L_0+1} p_j f_D(n-j), \quad 0 < n < L_0 + 1 \tag{14}$$

$$p_{L_0+1} = \sum_{j=0}^{L_0+1} p_j (\sum_{k \geq 0} f_D(L_0 + 1 - j + k)) \tag{15}$$

These equations can be written compactly as

$$\mathbf{p} = \mathbf{H}\mathbf{p}. \tag{16}$$

Thus, $\mathbf{p}$ is the eigenvector of $\mathbf{H}$ corresponding to eigenvalue 1. The discrete random process $\{C_m\}$ is a Finite State Markov Chain (FSMC). The states of the FSMC can be shown to be positive recurrent, and hence, a stationary distribution exists and it can be obtained by solving (16). The steady state distribution for $k = mT + l$ for $0 < l < T$ can be obtained as

$$f_{C_l}(c) = (f_C * \underbrace{f_A * f_A * \ldots * f_A}_{l \text{ times}})(c). \tag{17}$$

Notice that the stationary distribution of the fraction of compromised keys is independent of the size of the network. Clearly, the steady state distribution exists for the limiting case $L \to \infty$ and is identical to the distribution of C.

Now, the fraction of compromised links C can be related to the percolation threshold to obtain the outage probability. Let p_c be the percolation threshold for a given geometric graph. An outage occurs if $1 - C < p_c$, which indicates that the network does not have instantaneous connectivity. The outage probability is defined in (5) and it can be obtained using the distribution of C. The definition of outage probability combines two different aspects of the network: time-varying failures and recoveries through the queuing model, and geometry of the network through the percolation threshold. From a pure queuing perspective, we have a finite buffer, and the outage occurs whenever the queue length is larger than a *fraction* of the buffer size. This is motivated by the physical model of the network where the fraction of link compromises must not exceed a certain constant so that connectivity is present. From the percolation perspective, we obtain probability of instantaneous connectivity where the number of compromised keys evolves according to a queuing equation.

We do not have a closed form expression for the outage probability, although it can be obtained by solving for the distribution of C using (16). In Section IV, we will present numerical results to characterize the behavior of outage probability. We also note that we can obtain the exact distribution of the fraction of compromised links for a finite network, although the results from percolation theory will no longer hold. A heuristic definition of outage can be used in that case.

So far we have assumed that the key distribution mechanism successfully secures all the links and $p_{key} = 1$. The following remark shows how the situation with $p_{key} < 1$ can be handled.

Remark 1. *If the probability that two nodes share a private key $p_{key} < 1$, an outage in instantaneous connectivity occurs when $p_{key}(1-C) < p_c$, and hence, the analysis in this section holds with p_c replaced by p_c/p_{key}. Clearly, if $p_{key} < p_c$, $P_{outage} = 1$, i.e., connectivity does not exist even if there are no key compromises.*

B. Correlated failures in square lattices

Now, we present a simple model for correlated failures in a square lattice to show how our approach may be extended to a more general scenario where correlated failures may occur. We consider a square lattice shown in Fig. 2, where a legitimate node is present at each vertex of the lattice. Each node is connected to its nearest neighbors. It is assumed that each square region may contain an adversary. An adversary node results in correlated node or link failures in the lattice. For example, adversary node X_1 in Fig. 2 results in the failure of all the links of nodes a, b, c and d. Thus, the link compromises are correlated. This can also be considered as a correlated node failure where nodes a, b, c and d fail together. This can model physical capture of adjacent nodes, jamming by an active adversary, or eavesdropping and cryptanalysis carried out by a computationally powerful adversary. This approach can be extended to consider adversaries that lead to arbitrary node failures, or more powerful adversaries. For example, adversary node X_2 in Fig. 2 results in the failure of all nodes located on the vertices of the four squares around it.

Let L be the total number of square regions in the network. At time k, $A_k^{(L)}$ new adversaries appear in the network and are placed independently, and at time $k = mT$, failures corresponding to $B_{mT}^{(L)}$ adversaries are recovered. The queue is used to store the number of adversaries in the system. If $\{A_k^{(L)}\}$ and $\{B_{mT}^{(L)}\}$ are i.i.d., and we assume a linear scaling in L, we can use the results presented above to obtain the stationary distribution of the fraction of square regions that have an adversary. The percolation thresholds corresponding to these models of correlated failures are not known. Estimates of percolation thresholds for the model discussed above were obtained in [7], through simulations, and the outage probability can be estimated using those results. For example, if adversary nodes are similar to the adversary node X_1 in Fig. 2, and lead to failures of four nodes around them, the critical value of the fraction of squares containing an adversary was estimated as 0.163.

For arbitrary correlated failures, more intricate models that combine queuing models and percolation analysis are needed. Such models are beyond the scope of this paper, and will be explored in our future work.

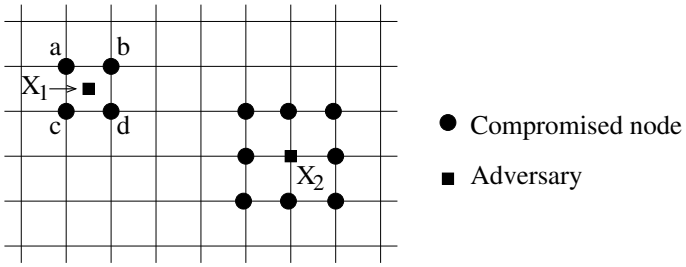


Fig. 2. Correlated failures in a square lattice

IV. Numerical Results

We now present numerical results on the outage probability. The stationary distribution of the fraction of keys compromised C is determined by solving (16). We plot the complementary cumulative distribution function (CCDF) of C for various parameters. The CCDF can be used to obtain the outage probability $\Pr\{C > 1 - p_c\}$, where p_c is the percolation threshold for the specific graph.

The distribution of C can be obtained for a general distributions f_A and f_B. For the numerical results, the distribution of A_k was assumed to be

$$A_k = \begin{cases} 0, & \text{w.p. } 0.8 \\ 0.001\alpha, & \text{w.p. } 0.1 \\ 0.002\alpha, & \text{w.p. } 0.1 \end{cases} \tag{18}$$

for $\alpha > 0$. It was assumed that $B_{mT} \in \{0, B_{max}\}$, and $B_{mT} = B_{max}$ w.p. p_{rec}, i.e., probability of recovery. p_{rec} is the probability that up to B_{max} compromised keys can be recovered successfully. With probability $1 - p_{rec}$ the recovery of compromised keys fails completely. A discretization corresponding to $L_0 = 10^3$ was assumed throughout.

Fig. 3 shows the CCDF of C for $\alpha = 5$, $B_{max} = 0.04$ and various values of p_{rec}. The values of $1 - p_c$ for square and triangular lattices are shown in the figure [15]. Here $T\mathbf{E}[A_k] = 0.36$, and hence, we must have $p_{rec} > 0.9$ to ensure that $\mathbf{E}[B_{mT}] > \mathbf{E}[A_k]$. Notice that a relatively high value of p_{rec} is required for obtaining a low outage probability. For example, for both the square and triangular lattices, the outage probability is more than 0.4 if $p_{rec} = 0.93$. A target outage probability of 10^{-4} requires $p_{rec} = 0.999$, while $p_{rec} = 0.99$ suffices for the triangular lattice. It was expected that a value larger than 0.9 would be needed for obtaining a low outage probability, however, the numerical results show that p_{rec} is required to be fairly close to 1. This result shows that it is critical that the key compromises are detected and recovered with high probability. Fig. 2 shows that the outage probability is far more sensitive to the probability of key recovery rather than the average rate of recovery. Thus, the average rate of key recovery is not a good metric if outage probability must be reduced. Similarly, Fig. 3 shows the effect of scaling the network for the same compromise and recovery processes, where the outage probability was expected to change with scaling, but not dramatically. The intuition obtained from these results is different than what one would obtain from a simple

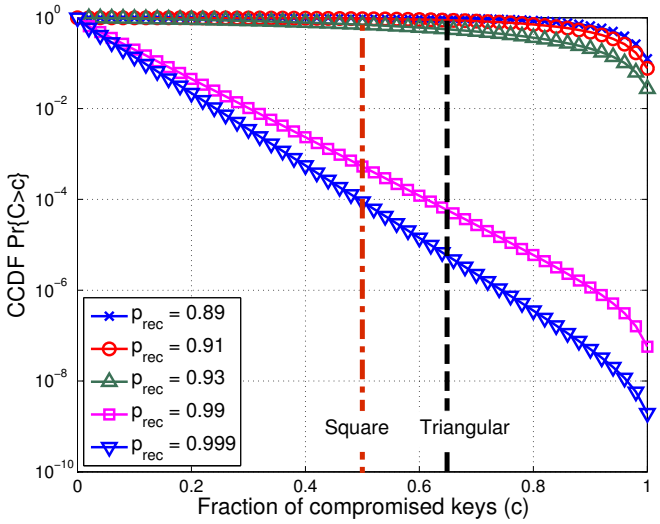


Fig. 3. Effect of p_{rec} on CCDF of fraction of keys compromised C

queuing analysis which ignores the geometry of the network. Such an analysis would perhaps require that the value of C be small.

In Fig. 3, B_{max} is kept constant, and hence, both p_{rec} and $\mathbf{E}[B_{mT}]$ increase with increase in p_{rec}. We now explore the effect of reliability in recovery of compromised links p_{rec} on the outage probability when the average number of recovered keys $\mathbf{E}[B_{mT}]$ remains constant. Fig. 4 shows the CCDF of C for $\alpha = 5$. Various combinations of B_{max} and p_{rec} were chosen so that the average number of recovered keys was kept fixed at $\mathbf{E}[B_{mT}] = 0.36$. Therefore, the same number of keys can be recovered on the average, in all the cases, and the amount of resources spent on key recovery is the same, on the average. The figure shows that for a fixed $\mathbf{E}[B_{mT}]$, an increase in the recovery probability p_{rec} results in a significantly lower outage probability. For $p_{rec} = 0.792$, the outage probability is more than 10^{-2} for both the square and triangular lattices, while for $p_{rec} = 0.99$, the outage probability for the square and triangular lattices is below 10^{-3} and 10^{-4}, respectively. Thus, while the average number of recovered keys has a weak influence on the outage probability, the recovery probability p_{rec} influences the outage probability very strongly.

Fig. 5 shows the effect of scaling of key compromise and recovery processes on the outage probability. The scaling was obtained by choosing different values of α, and choosing $B_{max} = 0.008\alpha$. Thus, the ratio $\mathbf{E}[A_k]/\mathbf{E}[B_{mT}]$ was kept fixed, while the fraction of keys compromised or recovered scales with α. p_{rec} was chosen to be 0.95. As α increases, the variability in links compromised or recovered increases and it is expected that the outage probability will increase. The increase in outage probability is substantial; as α is increased from 1 to 2, the outage probability for the triangular lattice increases by almost two order of magnitude. Thus, if the number of keys compromised per time unit remains the same, doubling the size of the network can dramatically reduce the

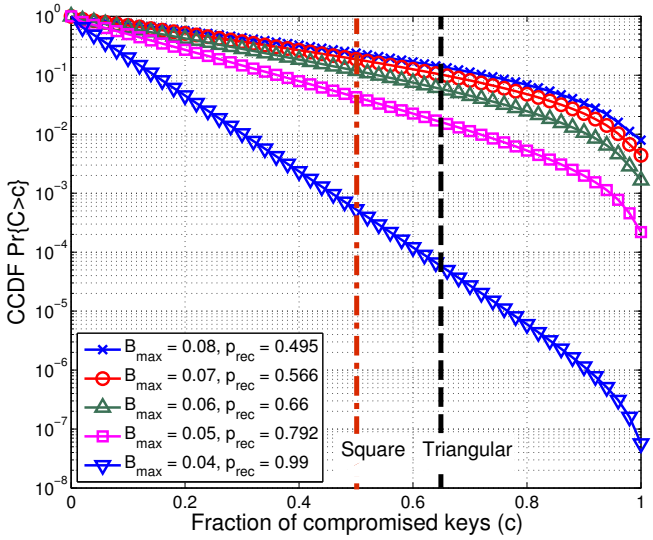


Fig. 4. Effect of p_{rec} on CCDF of fraction of keys compromised C for fixed $\mathbf{E}[B_{mT}]$

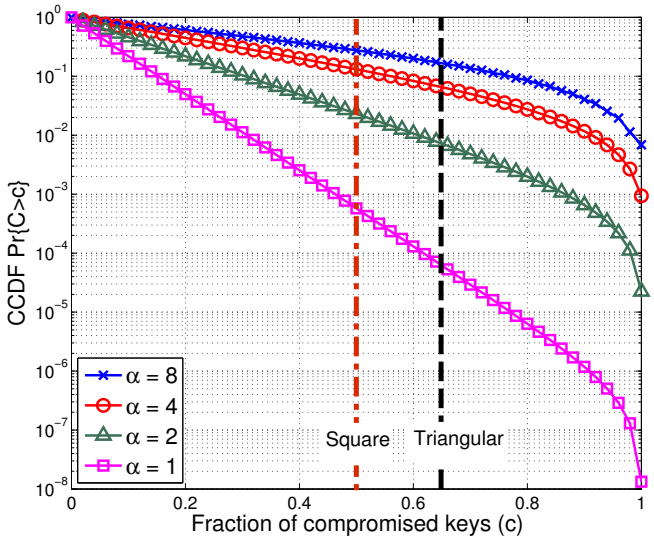


Fig. 5. Effect of scaling on CCDF of fraction of keys compromised C

outage probability. This also indicates that a smaller network will need a much smaller ratio of $\mathbf{E}[A_k]/\mathbf{E}[B_{mT}]$ compared to a larger network.

V. Conclusion

We have introduced a framework that models the dynamics of key compromise and recovery in a wireless network. The dynamic behavior was captured using a queuing model with a finite buffer, and the exact stationary distribution of the fraction of keys compromised was found. In particular, we modeled the uncertainty in the recovery of compromised keys. Outage probability was defined in terms of connectivity in large networks. The framework presented in this paper can also be used to model time-varying failures in a non-security setup. Numerical results showed that in order to obtain a low outage probability, recovery probability of compromised keys must be high. It was shown that the first order metric of average number of recovered keys is not sufficient. In this paper, we have used an i.i.d. model for both key compromise and recovery. A more realistic model will capture the spatial dependence of compromises in terms of correlated failure and recovery, and will be considered in our future work.

Acknowledgement

Research was sponsored by the U.S. Army Research Laboratory under the Network Science Collaborative Technology Alliance, Agreement Number W911NF-09-2-0053. The views and conclusions contained in this document are those of the author(s) and should not be interpreted as representing the official policies, either expressed or implied, of the U.S. Army Research Laboratory or the U.S. Government. The U.S. Government is authorized to reproduce and distribute reprints for Government purposes notwithstanding any copyright notation hereon.

References

[1] C. E. Perkins, *Ad Hoc Networking*. Addison-Wesley Professional, 2008.
[2] L. Eschenauer and V. Gligor, "A key-management scheme for distributed sensor networks," in *Proceedings of ACM Conference on Computer and Communications Security*, 2002, pp. 41–47.
[3] H. Chan, A. Perrig, and D. Song, "Random key predistribution schemes for sensor networks," in *Proceedings of IEEE Symposium on Security and Privacy*, 2003, pp. 197–215.
[4] D. Liu, P. Ning, and R. Li, "Establishing pairwise keys in distributed sensor networks," *ACM Transactions on Information and System Security*, vol. 8, no. 1, pp. 41–77, 2005.
[5] H. Chan, V. Gligor, A. Perrig, and G. Muralidharan, "On the distribution and revocation of cryptographic keys in sensor networks," *IEEE Transactions on Dependable and Secure Computing*, vol. 2, no. 3, pp. 233–247, 2005.
[6] M. Haenggi, "The secrecy graph and some of its properties," in *Proceedings of IEEE International Symposium on Information Theory*, July 2008, pp. 539–543.
[7] S. Goel, V. Aggarwal, A. Yener, and A. R. Calderbank, "Modeling location uncertainty for eavesdroppers: A secrecy graph approach," in *Proceedings of IEEE International Symposium on Information Theory*, 2010, pp. 2627–2631.
[8] M. A. Hamid and C. S. Hong, "A secure message percolation scheme for wireless sensor network," *Lecture Notes in Computer Science, Springer*, pp. 554–563, 2008.
[9] Z. Kong and E. M. Yeh, "Connectivity, percolation, and information dissemination in large-scale wireless networks with dynamic links," *submitted to IEEE Transactions on Information Theory*, 2009.
[10] P. De, Y. Liu, and S. K. Das, "Modeling node compromise spread in wireless sensor networks using epidemic theory," in *Proceedings of International Symposium on a World of Wireless, Mobile and Multimedia Networks*, 2006.
[11] M. E. Whitman and H. J. Mattord, *Principles of Information Security*. Thomson, Canada, 2009.
[12] S. R. Broadbent and J. M. Hammersley, "Percolation processes. I. Crystals and Mazes," in *Proceedings of the Cambridge Philosophical Society*, vol. 53, Jul. 1957, pp. 629–641.
[13] G. Grimmett, *Percolation*. Berlin: Springer-Verlag, 1999.
[14] L. Kleinrock, *Queuing systems: Vol. I*. New York: John Wiley and Sons, 1976.
[15] M. F. Sykes and J. W. Essam, "Exact critical percolation probabilities for site and bond problems in two dimensions," *Journal of Mathematical Physics*, vol. 5, no. 8, pp. 1117–1127, 1964.