# Control Channel Jamming: Resilience and Identification of Traitors

Agnes Chan, Xin Liu, Guevara Noubir, Bishal Thapa
College of Computer and Information Scinece
Northeastern University, Boston, MA 02115
ahchan, liux, noubir, bthapa@ccs.neu.edu

**Abstract**

In this paper, we address the problem of countering the control channel jamming in wireless communication systems. Targeting control traffic on a system like GSM (e.g., BCCH channel) leads to smart attacks that are four orders of magnitude more efficient than blind jamming. We propose several schemes based on coding theory and its applications that can counter both external and internal attackers (traitors). We introduce a T-(traitor) resilient scheme that requires less than $(T \log_T N)^2$ control information retransmissions and guarantees delivery of control information against any coalition of $T$ traitors. The proposed scheme also allows the identification of the traitors.

## I. Introduction

Signaling and control channels are essential to the operation of wireless communication networks. Such networks are constrained by the limited radio-frequency bandwidth and energy available to the mobile devices. Therefore, wireless networks implement various control mechanisms to conserve the limited resources. One of them is to employ shared control channels for sending system control information. For example, the GSM cellular communication system has multiple control channels for different functionalities [1], [2]. The broadcast channels (BCH), such as BCCH, SCH, and FCH, carry the network/cell identity, the structure of the current control channels and synchronization information. The common control channels (CCCH), such as AGCH, and PCH, are used for subscriber channel assignment and paging notification. A subscriber has to first lock to the appropriate channel of nearby base station by monitoring the broadcast control channels, send out connection requests to the base station and get an assignment of traffic channel before being able to initiate a call.

The BCH and some CCCH in GSM are located at very specific timeslots and physical frequency band (usually TS0 on a single 200KHz band) such that a subscriber can easily listen to them [2]. However, this makes the system vulnerable. An attacker can launch a denial of service attack by jamming the control channels. It is a highly energy efficient and effective attack for the attacker compared to jamming the whole frequency band to stop the communication. We simulate the scenario using Qualnet Simulator [3]. The result shows that by jamming 1 timeslot (out of 8 timeslots) of BCCH in every 51 frames on a single 200KHz band, the attack prevents all the mobile stations from communicating with each other. This leads to a jammer four order of magnitude more efficient than a jammer that is not aware of the GSM structure. Similarly, Hass et al. discover and study the attacks against control channels in Personal Communications Services (PCS) network [4].

In this paper, we address the problem of counter-jamming control channels in wireless systems. We propose a solution which instead of mapping the control channels to static locations (in terms of timeslot, frequency), it randomly maps them according to a cryptographic function. Such a mapping is unpredictable for an external attacker since it does not have the shared secret within the system. As a result, the external attacker will have to jam blindly which is either energy inefficient or less effective.

The above scheme prevents the external attacker from destroying the control channels, however, it cannot defeat the attack from a traitor inside the network. Any internal attacker will know the locations of the control channels and will be able to jam them. Therefore, we focus on designing schemes that are resilient to any coalition of $T$ traitors. A traitor is defined as a malicious user inside the system whose intention is to prevent the delivery of broadcast control information. The countermeasure includes two parts, (1) provide the network resilience against the traitor's attack, (2) identify the traitor and eliminate it from the system. In our context, the definition of resilience is the ability to send control messages successfully to all the users at least once during a bounded period of time even if there is a traitor within the system. We define $T$-resilient as a property of being resilient to $T$ traitors. Our main contribution is that we propose novel mechanisms to counter control channel jamming. Our schemes are resilient to any coalition of $T$ traitors. They also allow to identify the traitors.

**Related Work:** Wireless networks are highly sensitive to denial of service attacks [5], [6], [7], [8]. The broadcast nature of wireless communication exposes the physical layer of the system to jamming. The traditional anti-jamming strategy has been extensively relying on spread spectrum technique [9]. Very little work has been done from a system level to countermeasure jamming. In our previous work, we propose a novel system architecture based on mechanism-hopping to increase the wireless network robustness against cross-layer jamming [10]. Xu et al. study the effect and detection of jamming at MAC and PHY layer in wireless sensor networks in [11]. Geng et al. survey the denial of service attacks against wireless networks and propose a policy based networking framework to defend against DDoS for mobile systems [8]. Resilience and identification of internal attackers is very difficult. To the best of our knowledge, we are the first to investigate the problem of control channel jamming by traitors. We use results from coding theory to assign keys in our approach that guarantees the resilience and identification of traitors [12], [13].

The rest of the paper is organized as follows. In Section II, we present a scheme for a network with one traitor. In Section III, we present a solution when there are up to $T$ traitors in the network. Section IV concludes the paper.

## II. One Traitor Scheme

In this section, we consider a system where there is only one traitor among $N$ users. We present a 1-resilient scheme that requires $2\log_2 N$ replications of control information. This scheme also allows us to uniquely identify the jammer if any.

### A. The Scheme

We divide the communication time into periods, each consisting of $p$ timeslots. At each time slot, the system access information is sent over $q$ control channels. A user can access one and only one control channel in a timeslot using its corresponding key.

The key distribution phase is described in Algorithm 1. We call this 1-traitor distribution scheme Binary encoding based Key assignment (BBK). The scheme uses a key pool $F$ of $2\log_2 N$ keys. Each user is given $\log_2 N$ keys. The algorithm assigns a key to user $j$ at timeslot $i$ based on the $i^{th}$ bit of its binary encoding.

The algorithm uses a $N \times \log_2 N$ key distribution matrix $K$ to store the key assignment of each user. Each row $j$ in the matrix represents the $\log_2 N$ key assignment of user $j$ to be used during $\log_2 N$ timeslots respectively. For convenience, we denote $K_{ij}$ by $K_i^{(j)}$.

The control information transmission procedure is described in Algorithm 2. At each time slot, the system generates two control signals. The channels at time slot $i$ are determined by two functions: $f(k_i, i)$ and $f(k_i^{'}, i)$, where $f$ is a publically known cryptographic hashing function. User $j$ knows the location

**Algorithm 1**: BBK

**Setup:** $N$ users, 1 traitor.

**Result**: distribution matrix $K = (K_i^{(j)})_{N \times \lceil \log_2 N \rceil}$.

**begin**

$F = \{k_1, k_2, \cdots, k_{\lceil \log_2 N \rceil}, k_1^{'}, k_2^{'}, \cdots, k_{\lceil \log_2 N \rceil}^{'}\}$

**for** *j = 0* **to** $N - 1$ **do**

$j \leftarrow (j_1 j_2 \cdots j_{\lceil \log_2 N \rceil})$ // binary encoding

**for** *i=1* **to** $\lceil \log_2 N \rceil$ **do**

$$K_i^{(j)} = \begin{cases} k_i, & if \quad j_i = 0 \\ k_i^{'}, & if \quad j_i = 1 \end{cases}$$

Assign keys from $j^{th}$ row of $K$ to user $j$

**end**

**Algorithm 2**: Transmission for One Traitor Case

**System Server:**

$i \leftarrow 1$

**for** *timeslot* $i$ **do**

Channel-send$_1$ = $f(k_{(i \bmod \lceil \log_2 N \rceil)}, i)$

Channel-send$_2$ = $f(k^{'}_{(i \bmod \lceil \log_2 N \rceil)}, i)$

Send control information on two channels

$i \leftarrow i + 1$

**User: For each user** $j \in \{0, 1, \cdots, N-1\}$

$i \leftarrow 1$

**for** *timeslot* $i$ **do**

Channel-listen = $f(K^{(j)}_{(i \bmod \lceil \log_2 N \rceil)}, i)$

$j$ listens to that channel

$i \leftarrow i + 1$

of control signal at time slot $i$ by computing $f(K^{(j)}_{(i \bmod \lceil \log_2 N \rceil)}, i)$. The server computes a $f$-table that stores the mapping of keys to channels at each timeslot. A legitimate user will succeed in accessing the control channel in a timeslot if no traitor jams that channel.

### *B. An Example*

Let us look at a wireless network with 8 users as an example. Following BBK, the key pool has 6 keys. Let $F = \{k_1, k_2, k_3, k_1^{'}, k_2^{'}, k_3^{'}\}$. In each timeslot the control information is sent out at 2 control channels determined by $f(k_i, i)$ and $f(k_i^{'}, i)$. Table I describes the key assignment to users. Notice that no traitor can jam a user throughout a period. For example, user 6 will listen to control channels $f(k_1, 1)$,$f(k_2^{'}, 2)$ and $f(k_3^{'}, 3)$ in timeslot $1, 2, 3$ respectively. Assume user 5 is the traitor, it knows and jams the location of $f(k_1^{'}, 1)$,$f(k_2, 2)$ and $f(k_3^{'}, 3)$. Although user 6 cannot access the control channels in timeslot 1 and 3 due to jamming of the traitor, it can still access the control channel at timeslot 2 as shown in the Figure 1. As a result, the system guarantees that each user gets access to the control channel in every 3 timeslots.

| Node | Bit-Representation | Key Assignment |
|---|---|---|
| 0 | 000 | $k_1\ k_2\ k_3$ |
| 1 | 100 | $k_1^{'}\ k_2\ k_3$ |
| 2 | 010 | $k_1\ k_2^{'}\ k_3$ |
| 3 | 110 | $k_1^{'}\ k_2^{'}\ k_3$ |
| 4 | 001 | $k_1\ k_2\ k_3^{'}$ |
| 5 | 101 | $k_1^{'}\ k_2\ k_3^{'}$ |
| 6 | 011 | $k_1\ k_2^{'}\ k_3^{'}$ |
| 7 | 111 | $k_1^{'}\ k_2^{'}\ k_3{}'$ |

TABLE I

KEY ASSIGNMENT FOR A 8-USER NETWORK WITH ONE TRAITOR.

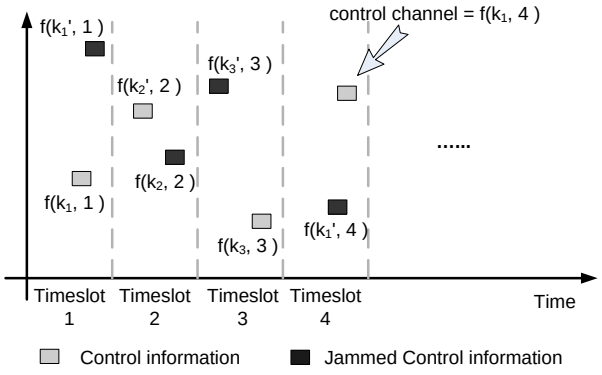


Fig. 1. Channel mapping for the 8-user network example. User 5 is the traitor. Network is 1-resilient.

### C. Correctness

*Theorem 1:* The BBK scheme is 1-resilient.

*Proof:* Let $t \in \{0, 1, \cdots, N-1\}$ be the traitor and $(t_1 t_2 \cdots t_{\lceil \log_2 N \rceil})$ be its binary encoding. Let $u \in \{0, 1, \cdots, N-1\} - \{t\}$ be any user with a binary encoding $(u_1 u_2 \cdots u_{\lceil \log_2 N \rceil})$. Then there must exist some $i, 1 \leq i \leq \lceil \log_2 N \rceil$ such that $t_i \neq u_i$ since $t \neq u$. From Algorithm 1, this guarantees that at timeslot $i$, $K_i^{(u)} \neq K_i^{(t)}$. Hence, the channel assignment $f(K_i^{(u)}, i) \neq f(K_i^{(t)}, i)$. Therefore, $u$'s access couldn't be jammed by traitor $t$ for $t$ doesn't know the location of control channel that $u$ listens to at timeslot $i$. Hence, BBK is 1-resilient. ■

### D. Traitor Identification

*Theorem 2:* If a traitor $t$ always jams, then BBK uniquely identifies $t$ .

*Proof:* Given that $t$ jams throughout the period of $\lceil \log_2 N \rceil$ timeslots, system knows all the $\lceil \log_2 N \rceil$ channels it jams. These channels correspond to a unique key assignment in the $f$-table. Then, from Algorithm 1, the system gets the binary encoding of $t$, and identify the traitor. ■

### E. An Alternate Strategy

We propose an alternate scheme based on combinatorial facts to provide resilience to the traitor. Resilience requires that no key assignment of a user is contained in another. The set of such assignments

forms an antichain [1]. Sperner's theorem proves that choosing all possible $\lfloor \frac{|F|}{2} \rfloor$-subset of $|F|$ gives the largest antichain of F [14].

*Key Distribution:* Given $N$, pick $F$ such that $N \leq \binom{|F|}{\lfloor \frac{|F|}{2} \rfloor}$. Let $K$ be the collection of all possible $\lfloor \frac{|F|}{2} \rfloor$-key sets out of the key pool $F$. Obviously, $K$ is an antichain. Then assign each user a unique element of $K$. This key assignment guarantees the resilience against the traitor. The proof is similar to that of BBK.

*Transmission:* The communication time is divided into periods, each consisting of $|F|$ timeslots. At timeslot $i$, the server sends control information over 1 control channel which is $f(K_{i \bmod |F|}, i)$. One user listens to $\lfloor \frac{|F|}{2} \rfloor$ timeslots whose indices equal to the indices of its keys.

This method allows more users to the system without increasing $F$ compared to BBK.

## III. Multiple Traitors Scheme

The BBK scheme described in Section II is good for the network where there is only one traitor. However, it may fail if there are multiple traitors in the network. For instance, in Table I, if user 1 and 7 are traitors, their keys combination covers the whole key pool. Therefore, the traitors know the locations of all the control channels and can totally block the legitimate users from accessing the control channels.

In this section, we introduce a scheme that is resilient to any coalition of $T$ traitors. The scheme guarantees that each legitimate user succeeds in accessing the control channel at least once during a period less than $T \log_T N$ timeslots. The scheme requires at most $(T \log_T N)^2$ retransmissions of the control information. Also, we present a solution to identify the traitors based on the system observation of the channels being jammed.

### A. The Scheme

We denote the scheme for multiple traitors scenario as Polynomial Based Key assignment for T traitors (PBK-T). Similar to the scheme for the one traitor case, the communication is divided into time periods, each consists of $p$ timeslots. In each timeslot, the control information is sent over $q$ different control channels.

The key distribution phase is described in Algorithm 3. The key pool $F$ consists of $p \times q$ keys. Let $F = \{k_0^{(0)}, \cdots, k_{p-1}^{(0)}, k_0^{(1)}, \cdots, k_{p-1}^{(1)}, \cdots, k_0^{(q-1)}, \cdots, k_{p-1}^{(q-1)}\}$. Each registered user is assigned $p$ keys. The system administrator identifies the users by assigning each a unique polynomial over $GF(q)$ with degree $\leq c$. Let $u_j(x) = \sum_{k=0}^{c} s_k^{(j)} x^k$ denote the identifying polynomial of user $j$ , and $s_j = (s_0^{(j)}, s_1^{(j)}, \cdots, s_c^{(j)})$ be its coefficient vector. Evaluating $u_j(x)$ over $\{0, 1, \cdots, p-1\}$ gives $p$ values in GF(q), and the values are used by the system for key assignment to user $j$.

The control information transmission procedure is described in Algorithm 4. In timeslot $i$, the control channels that the control information is sent over are determined by $f(K_{i \bmod p}^{(j)}, i)$, $\forall j \in \{0, \cdots, q-1\}$, where function $f$ is a known cryptographic hashing function. A user knows one of the control channels in timeslot $i$ by computing $f(K_{i \bmod p}^{(j)}, i)$. The server keeps $f$-table that maps a key assignment to a unique channel assignment similar to that of BBK scheme.

### B. Correctness

*Theorem 3:* The PBKA-T scheme is T-resilient if the following properties are satisfied:

[1]A is an antichain in $F$ iff it is a collection of nonempty subsets of $F$ such that no element of $A$ is contained in another element of $A$

**Algorithm 3**: PBK-T

**Setup:** $N$, key pool $F$
**Result:** a $N \times p$ key-distribution matrix $K$ noted $K_{ji}$ or $K_i^{(j)}$
**begin**
  Initialize $K \leftarrow [0]_{N \times p}$
  S = { (c+1)-vector in GF(q) }
  **for** *j = 0* **to** $N-1$ **do**
    Pick unique $s_j \in S$
    **for** *i = 0* **to** $p-1$ **do**
      $\gamma = \sum_{k=0}^{c} s_k^{(j)} i^k$
      $K_i^{(j)} = k_i^{(\gamma)}$
  Send $\{K_0^{(j)}, K_1^{(j)}, \cdots, K_{p-1}^{(j)}\}$ to user $j$
**end**

**Algorithm 4**: Transmission for Multi-Traitor Case

**System Server:**
$i \leftarrow 1$
**for** *timeslot i* **do**
  $l = i \bmod p$
  **for** *j = 0* **to** $q-1$ **do**
    Channel-send = $f(K_l^{(j)}, i)$
    Send access information on this channel
  $i \leftarrow i+1$
**User: for user** $j \in \{0, 1, \cdots, N-1\}$
$i \leftarrow 1$
**for** *timeslot i* **do**
  $l = i \bmod p$
  Channel-listen = $f(K_l^{(j)}, i)$
  Listen to that channel
  $i \leftarrow i+1$

$$q^{c+1} \geq N \tag{1}$$

$$q \geq p \tag{2}$$

$$p > T \times c \tag{3}$$

*Proof:* Inequality 4 guarantees that there are sufficient distinct polynomials over GF(q) with degree $\leq c$ for $N$ users.

If Inequality 2 is not satisfied, which means $p > q$, evaluating the identifier polynomial $u_j(x)$ over $\{0, 1, \cdots, p-1\}$ is equivalent to evaluating the polynomial over $\{0, 1, \cdots, q-1, 0, 1, \cdots, (p-1) \bmod q\}$, hence, the length of the time period shrinks to $q$ timeslots.

Since two polynomials of degree $\leq c$ cannot be equal over more than $c$ points without being identical,

two users have at most $c$ keys in common. Therefore, the combination of all the keys of $T$ traitors can coincide with at most $Tc$ keys of any other user. Thus, Inequality 3 guarantees that for any user there exists at least one key different from that of any $T$ other users combined. After the mapping, for any legitimate user, there is at least one control channel that it listens to, during a period of $p$ timeslots, not jammed by the traitors. This proves that the PBK-T scheme is T-resilient. ■

### C. Performance Analysis

One objective of our scheme is to minimize the number of control message retransmissions or to reduce the key pool size.

*Theorem 4:* For a PBK-T problem, where $N > 1$, $T \geq 1$, and $N > T$, the optimal solution, $F_{OPT}$ has:

$$\begin{cases} |F|_{OPT} \leq \max((\lceil \ln N \rceil)^2, \lceil e \rceil \lceil \ln N \rceil), & when \;\; T = 1; \\ |F|_{OPT} = N, & when \;\; T \geq \sqrt{N} - 1; \\ |F|_{OPT} < (T \lceil \frac{\ln N}{\ln T} \rceil)^2, & when \;\; 1 < T < \sqrt{N} - 1. \end{cases}$$

Please refer to the Appendix for the proof.

### D. An Example

Consider a wireless network with 9 users and 2 traitors as an example. We pick $q = p = 3$ and $c = 1$ such that both Inequality 4 and 3 are satisfied. Thus the key pool has $|F| = 9$ keys. Let $F = \{k_0^0, k_0^1, k_0^2, k_1^0, k_1^1, k_1^2, k_2^0, k_2^1, k_2^2\}$. In each timeslot, the system information is sent out at 3 control channels determined by $f(k_{i \bmod 3}^0, i), f(k_{i \bmod 3}^1, i)$ and $f(k_{i \bmod 3}^2, i)$. The key assignment is illustrated in Table II. Notice that no two traitors can jam any other user at all timeslots.

| Node $j$ | Polynomial Identifier | Eval $u_j(0)$ | Eval $u_j(1)$ | Eval $u_j(2)$ | Key Assignment |
|---|---|---|---|---|---|
| 0 | 0 | 0 | 0 | 0 | $k_0^0\ k_1^0\ k_2^0$ |
| 1 | 1 | 1 | 1 | 1 | $k_0^1\ k_1^1\ k_2^1$ |
| 2 | 2 | 2 | 2 | 2 | $k_0^2\ k_1^2\ k_2^2$ |
| 3 | $x$ | 0 | 1 | 2 | $k_0^0\ k_1^1\ k_2^2$ |
| 4 | $1+x$ | 1 | 2 | 0 | $k_0^1\ k_1^2\ k_2^0$ |
| 5 | $2+x$ | 2 | 0 | 1 | $k_0^2\ k_1^0\ k_2^1$ |
| 6 | $2x$ | 0 | 2 | 1 | $k_0^0\ k_1^2\ k_2^1$ |
| 7 | $1+2x$ | 1 | 0 | 2 | $k_0^1\ k_1^0\ k_2^2$ |
| 8 | $2+2x$ | 2 | 1 | 0 | $k_0^2\ k_1^1\ k_2^0$ |

TABLE II

KEY ASSIGNMENT FOR A 9-NODE NETWORK WITH 2 TRAITORS.

### E. Traitors Identification

*Theorem 5:* The PBK-T identifies any $T$ traitors.

*Proof:* Let $C = \{C^{(1)}, C^{(2)}, \cdots, C^{(p)}\}$ be a set of sets $C^{(i)}$ such that each $C^{(i)}$ represents a set of channels jammed at timeslot $i$ by a coalition of $T$ traitors. We know that $|C^{(i)}| \leq T \ \forall i$. We construct a set S such that it consists of all possible combinations of jammed channels by picking a channel from each $C^{(i)}$. Let $S = \{(s_1\ s_2\ \cdots\ s_p) | s_i \in C^{(i)}\}$. Since $f$ is a cryptographic hashing function (injective with high probability), each element of $S$ corresponds to a unique key assignment in $f$-table. We call an element of $S$ valid if it matches the channel assignments of one user.

Assume there are $T+R$ valid elements in $S$ such that $R>0$. This implies, there exists $R$ users whose access to control channels are being jammed by $T$ traitors. Thus, the system is not $T$-resilient. This is in contradiction with Theorem 3. Therefore, $R$ must be 0. Every valid element of $S$ corresponds to a traitor's key assignment in $f$-table and the key assignment corresponds to its identity in the key distribution matrix $K$. Hence, PBK-T identifies all the traitors. ■

*Performance:* The identification of $T$ traitors require $T^{(c+1)}$ $f$-table lookups where $c$ is the maximum degree of identifying polynomials. Since, any valid channel assignment will have at most $c$ common assignments, checking $T^{(c+1)}$ possible candidates will result in identifying all $T$ traitors.

## IV. Conclusion

We introduce a novel T-resilient scheme that requires at most $(T\log_T N)^2$ control information retransmission to guarantee the delivery of such information to all users against any coalition of $T$ traitors. The proposed scheme also allows the identification of the traitors. Our next step is to extend the combinatorial method for the multiple traitor case. It will be interesting to investigate the scheme which assigns different number of keys to different users and analyze its performance. Also we plan to study the lower bound of key pool size.

## V. Appendix

In this section, we discuss the key pool size $|F|$ of PBK-T. We assume that $N>1$, $T\geq 1$, and $N>T$, (otherwise it is meaningless to study the traitor problem). From Theorem 3, we know that a correct solution of PBK-T must satisfy the following properties:

$$q^{c+1}\geq N \tag{1}$$

$$q\geq p \tag{2}$$

$$p\geq T\times c+1 \tag{3}$$

*Theorem 4:* For a PBK-T problem, where $N>1$, $T\geq 1$, and $N>T$, the optimal solution, $F_{OPT}$ has:

$$\begin{cases} |F|_{OPT}\leq \max((\lceil \ln N\rceil)^2, \lceil e\rceil\lceil \ln N\rceil), & when \quad T=1; \\ |F|_{OPT}=N, & when \quad T\geq \sqrt{N}-1; \\ |F|_{OPT}<(T\lceil \frac{\ln N}{\ln T}\rceil)^2, & when \quad 1<T<\sqrt{N}-1. \end{cases}$$

*Proof:*

**Case one,** $T=1$**.** We have $|F|=p\times q\geq N^{\frac{1}{c+1}}(c+1)$. Let $f(c)=N^{\frac{1}{c+1}}(c+1)$. The function $f(c)$ is minimized when $c=c_1$ where $f'(c_1)=0$.

$$\begin{aligned} & f'(c)=N^{\frac{1}{c+1}}(1-\frac{\ln N}{c+1}) \\ \Rightarrow \quad & c_1=\ln N-1 \end{aligned}$$

$c_1$ is the local minimum since:

$$\begin{aligned} & f''(c)=N^{\frac{1}{c+1}}\ln N\frac{1}{(c+1)^2}(2-\frac{\ln N}{c+1}) \\ \Rightarrow \quad & f''(c=c_1)=N^{\frac{1}{c+1}}\ln N\frac{1}{(c_1+1)^2}>0 \end{aligned}$$

Let $c'=\lceil c_1\rceil$, since $c$ is the degree of the identifying polynomials therefore must be an integer.Set $p=c'+1=\lceil \ln N\rceil$, and $q=\max(\lceil e\rceil,p)$. Since $c'\geq c_0$, $N^{\frac{1}{c'+1}}<N^{\frac{1}{c_1+1}}=e$. Therefore $q\geq N^{\frac{1}{c'+1}}$,

and this is a feasible solution as it satisfies all the three properties in Theorem 3. As a result, $|F|_{OPT} \leq |F|_{c=c'} = \max((\lceil \ln N \rceil)^2, \lceil e \rceil \lceil \ln N \rceil)$.

**Case two,** $T \geq \sqrt{N} - 1$**.** Since $q \geq p$, $|F| = p \times q \geq p^2$. The valid $c$ is an integer.
If $c = 0$, $p = 1$, $q = N$, $\Rightarrow |F| = N$;
If $c \geq 1$, $p \geq \sqrt{N}$, $\Rightarrow |F| \geq (\sqrt{N})^2 = N$.
Therefore, $|F|_{OPT} = N$.

**Case three,** $1 < T < \sqrt{N} - 1$**.** Let $c_0$ be the point where $N^{\frac{1}{c_0+1}} = Tc_0 + 1$. As shown in Figure 2, $q$ is a monotonic decreasing function of $c$ with $\lim_{c\to\infty} q = 0$, and $p$ is a monotonic increasing function of $c$ with $\lim_{c\to\infty} q = \infty$. Since $q_{|c=0} = N > 1 = p_{|c=0}$, there must exist a $c_0$ where $q_{|c=c_0} = p_{|c=c_0}$.

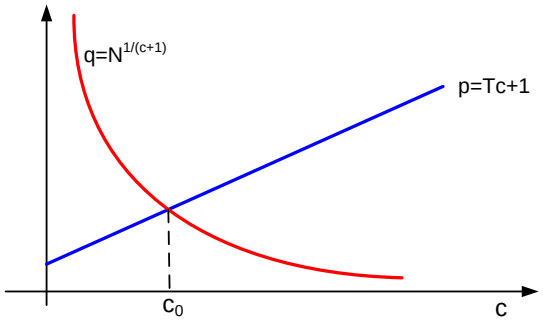


Fig. 2. p(c) and q(c)

In the following, we show that $1 < c_0 < \ln N / \ln T - 1$,
if $c_0 = 1$, $N^{\frac{1}{c_0+1}} = \sqrt{N}$, $Tc_0 + 1 = T + 1 < \sqrt{N}$, therefore, $c_0$ cannot be 1;
if $c_0 < 1$, $N^{\frac{1}{c_0+1}} > \sqrt{N}$, $Tc_0 + 1 < T + 1 < \sqrt{N}$, therefore, $c_0$ cannot be less than 1;

$$\begin{aligned} & N^{\frac{1}{c_0+1}} = Tc_0 + 1 > Tc_0 \\ \Rightarrow \quad & \frac{1}{c_0+1} \ln N > \ln Tc_0 \\ \Rightarrow \quad & \frac{\ln N}{\ln Tc_0} > (c_0 + 1) \quad (\because \ln Tc_0 > 0) \\ \Rightarrow \quad & c_0 < \frac{\ln N}{\ln T} - 1 \quad (\because c_0 > 1) \end{aligned}$$

Let $c' = \lceil c_0 \rceil$, as $c_0$ might not be an integer. Set $q = p = Tc' + 1$. Since $c' \geq c_0$, we have $q = Tc' + 1 \geq N^{\frac{1}{c'+1}}$. It is easy to verify that this is a feasible solution of PBK-T since it satisfies all the three properties in Theorem 3. The key pool size $|F|$ is bounded as follows:

$$\begin{aligned} |F| &= (Tc' + 1)^2 \\ &< (T\lceil \frac{\ln N}{\ln T} - 1 \rceil + 1)^2 \\ &< (T\lceil \frac{\ln N}{\ln T} \rceil)^2 \end{aligned}$$

Therefore, the optimal solution in the case has $|F|_{OPT} < (T\lceil\frac{\ln N}{\ln T}\rceil)^2$. ■

*Theorem 6:* The optimal solution of PBK-T, where $1 < T < \sqrt{N} - 1$, is

$$\min(N^{\frac{1}{\lfloor c_0 \rfloor + 1}}(T\lfloor c_0 \rfloor + 1), (T\lceil c_0 \rceil + 1)^2),$$

where $c_0$ is the point at which $N^{\frac{1}{c_0+1}} = Tc_0 + 1$.

*Proof:* As shown in Figure 2, when $c \in [0, c_0]$, $q = N^{\frac{1}{c+1}}$ and $p = Tc + 1$ are feasible solutions; when $c \in (c_0, \infty]$, we have to increase $q$ to $q = p = Tc + 1$ to be a feasible solution. Since $c \in [c_0, \infty]$, $p \times q = (Tc+1)^2 \geq (Tc_0+1)^2$, $|F|$ will be minimized at $c_0$ in this range. In the following, we discuss the case when $c \in [0, c_0]$.

Let $f(c) = p \times q = (Tc + 1)N^{\frac{1}{c+1}}$. The two roots of $f'(c) = 0$ are:

$$f'(c) = N^{\frac{1}{c+1}}(T - \frac{Tc+1}{(c+1)^2}\ln N) = 0$$

$$\Rightarrow \begin{cases} c_1 = (\frac{\ln N}{2} - 1) - \sqrt[2]{(\frac{\ln N}{2} - 1)^2 + (\frac{\ln N}{T} - 1)} \\ c_2 = (\frac{\ln N}{2} - 1) + \sqrt[2]{(\frac{\ln N}{2} - 1)^2 + (\frac{\ln N}{T} - 1)} \end{cases}$$

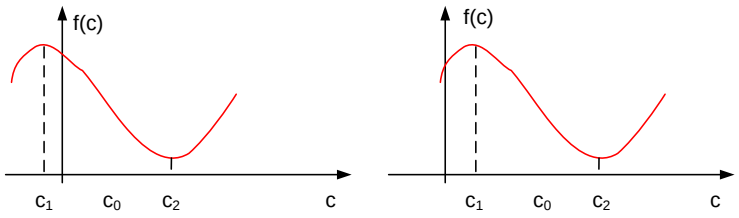


Fig. 3. $f(c) = p \times q$

1) Let $y = (\frac{\ln N}{2} - 1)^2 + (\frac{\ln N}{T} - 1) = \ln N(\frac{\ln N}{4} + \frac{1}{T} - 1)$,

$$T < \sqrt{N} - 1$$
$$\Rightarrow \quad y > \ln N(\frac{\ln N}{4} + \frac{1}{\sqrt{N} - 1} - 1)$$
$$\Rightarrow \quad y > 0 \ (\because \min(\frac{\ln N}{4} + \frac{1}{\sqrt{N} - 1} - 1) \approx 0.0245, when\ N = (2 + \sqrt{3})^2)$$

Therefore, $c_1$ and $c_2$ are real values.

2) Among the two critical points, $c_2$ is the local minimum point of $f(c)$, since

$$f''(c) = -\frac{TN^{\frac{1}{c+1}}\ln N}{(c+1)^2} + \frac{2f(c)\ln N}{(c+1)^3} - \frac{f'(c)\ln N}{(c+1)^2}$$

$$\Rightarrow \quad f''(c_2) = \frac{2(Tc_2+1)N^{\frac{1}{c_2+1}}\ln\ (\because f'(c_2) = 0)N}{(c_2+1)^3} - \frac{TN^{\frac{1}{c_2+1}}\ln N}{(c_2+1)^2}$$

$$= \frac{N^{\frac{1}{c_2+1}}\ln N}{(c_2+1)^3}(Tc_2 - T + 2)$$

$$> 0 \ (\because\ when\ N > 5,\ c_2 > 1 \Rightarrow (Tc_2 - T) > 0;\ when\ T < N \leq 5, Tc_2 - T + 2 > 0\ )$$

3) We would like to show that $c_1 < c_0 < c_2$. We know that $1 \leq c_0 < \frac{\ln N}{\ln T + \ln c_0} - 1$ in Theorem 4. Thus, as long as we prove that $c_1 \leq 1$ and $c_2 \geq \frac{\ln N}{\ln T + \ln c_0} - 1$, we are done.

3.1) Proof of $c_1 < 1 < c_0$

i) If $\frac{\ln N}{T} \geq 1$, then $c_1 \leq 0$, therefore done.

ii) Else if $0 < \frac{\ln N}{T} < 1$

$$\begin{aligned} & -1 < \frac{\ln N}{T} - 1 < 0 \\ \Rightarrow \quad & \frac{\ln N - 2}{2} - 1 < \sqrt{(\frac{\ln N - 2}{2})^2 + (\frac{\ln N}{T} - 1)} < \frac{\ln N - 2}{2} \\ \Rightarrow \quad & 0 < (\frac{\ln N}{2} - 1) - \sqrt{(\frac{\ln N}{2} - 1)^2 + (\frac{\ln N}{T} - 1)} < 1 \\ \Rightarrow \quad & 0 < c_1 < 1 < c_0 \end{aligned}$$

3.2) Proof of $c_2 \geq \frac{\ln N}{\ln T + \ln c_0} - 1 \geq c_0$. We need to show

$$\frac{\ln N}{2} + \sqrt{(\frac{\ln N}{2} - 1)^2 + (\frac{\ln N}{T} - 1)} \geq \frac{\ln N}{\ln T + \ln c_0} \tag{4}$$

i) If $Tc_0 \geq 8 > e^2 \Rightarrow \ln T + \ln c_0 >= 2$, we are done.

ii) Else if $Tc_0 \leq 7$, we have

| $c_0$ | T | N | Left-Side of (4) | Right-Side of (4) |
|---|---|---|---|---|
| 1 | 1 | 4 | 1.39 | - |
| 1 | 2 | 9 | 1.43 | 3.17 |
| 1 | 3 | 16 | 1.66 | 2.52 |
| 1 | 4 | 25 | 2.03 | 2.32 |
| 1 | 5 | 36 | 2.38 | 2.23 |
| 1 | 6 | 49 | 2.68 | 2.17 |
| 1 | 7 | 64 | 2.95 | 2.14 |
| 2 | 1 | 8 | 2.08 | 3 |
| 2 | 2 | 64 | 3.58 | 3 |
| 2 | 3 | 216 | 4.56 | 3 |
| 3 | 1 | 81 | 4.4 | 4 |
| 3 | 2 | 1296 | 6.63 | 4 |

TABLE III

Table III shows only when N is very small ($N \leq 25$), the Inequality 4 does not hold. For a network with a large number of users ($N > 25$), Inequality 4 is always true. Actually, to reduce the key pool size of large size networks are more valuable and interesting to us. The goal of our design is to reduce of key pool size for large size networks. Therefore, for a large size network ($N > 25$), $c_0 < c_2$.

4) From 1)∼3), we get: when $c \in [c_1, c_0]$, $f(c_0) < f(c)$; when $c \in [0, c_1]$, the only feasible choice is $c = 0$ and $|F| = N$, since $c$ has to be an integer.

As a conclusion, if $c_0$ is an integer, $c_0$ minimizes $f(c) = p \times q$ when $c \in [0, c_0]$ and $p^2$ when $c \in (c_0, \infty)$. Therefore, $|F|_{OPT} = (Tc_0 + 1)^2$. Otherwise,

$$|F|_{OPT} = \min(N^{\frac{1}{\lfloor c_0 \rfloor + 1}}(T\lfloor c_0 \rfloor + 1), (T\lceil c_0 \rceil + 1)^2).$$

■

## VI. DELAY

We described our scheme with:

- $p$ timeslots
- $q$ sub-channels
- $T$ or $t$ traitors
- $q \geq p$

We want to calculate the average delay of the scheme before an user is guaranteed a successful access of the channel. Basically, this happens when the combination of $t$ channels couldnt jam the $j$th channel of user $j$ at a timeslot $i$. So, the delay for each user is the timeslot at which they access the channel. If we consider the timeslot as a random variable with a probability distribution $P$, then its expected value is the average delay of the scheme.

We know that, at each timeslot $i \in \{1, 2, \cdots p\}$ the probability that an user gets an access to the channel is $(1 - \frac{t}{q})$ and the probability that it doesnt get an access is $(\frac{t}{q})^{i-1}$. Hence, Average Delay:-

$$E[i] = \sum_{i=1}^{p} i * (1 - \frac{t}{q}) * (\frac{t}{q})^{i-1}$$

Note that at $p$th timeslot, the probability that an user gets an access to the channel, given that it didnt get access until $(p-1)$th timeslot is 1. Hence,

$$\begin{aligned} E[i] &= \sum_{i=1}^{p-1} i * (1 - \frac{t}{q}) * (\frac{t}{q})^{i-1} + p * (\frac{t}{q})^{p-1} \\ &= 1 - \frac{t}{q} + 2(\frac{t}{q}) - 2(\frac{t}{q})^2 + 3(\frac{t}{q})^2 - 3(\frac{t}{q})^3 \cdots \\ &\quad + p(\frac{t}{q})^{p-2} - p(\frac{t}{q})^{p-1} + p(\frac{t}{q})^{p-1} \\ &= 1 + (\frac{t}{q}) + (\frac{t}{q})^2 + \cdots + (\frac{t}{q})^{p-2} \end{aligned}$$

This is a geometric series with $(p-1)$ elements and common ratio $(\frac{t}{q})$. Therefore

$$E[i] = \frac{1 - (\frac{t}{q})^p}{1 - (\frac{t}{q})}$$

If $p$ is very large, $E[i]$ becomes $[\frac{q}{q-t}]$.
If $p = 1$, $E[i]$ becomes 1. Hence

$$1 \leq \frac{1 - (\frac{t}{q})^p}{1 - (\frac{t}{q})} \leq [\frac{q}{q-t}]$$

**Claim:** $[\frac{q}{q-t}] \leq 2$.

*Proof:* We know, $q \leq tlog_t N$, where $N$ is the number of users in the network. Thus,

$$\frac{q}{q-t} \leq \frac{tlog_t N}{tlog_t N - t}$$

$$= \frac{log_t N}{log_t N - 1}$$

But, our hypothesis says $N \geq t^2$. So, $log_t N \geq 2$. Then

$$log_t N - 1 \geq log_t N - \frac{log_t N}{2}$$

.

$$\Rightarrow \frac{log_t N}{log_t N - 1} \leq \frac{log_t N}{\frac{log_t N}{2}} = 2$$

Hence,

$$\frac{q}{q-t} \leq 2$$

■

Therefore, the average delay of the scheme is between 1 to 2 timeslots.

## REFERENCES


[1] T. S. Rappaport, *Wireless Communications: Principles and Practice*. Prentice Hall, 1996.

[2] G. Heine, *GSM Networks: Protocols, Terminology, and Implementation*. Artech House Publisher, 1999.

[3] Scalable Network Technologies, http://www.scalable-networks.com.

[4] Z. J. Haas and Y.-B. Lin, "Demand re-registration for pcs database restoration," in *Proceedings of IEEE MILCOM*, 1999.

[5] G. Lin and G. Noubir, "On link layer denial of service in data wireless lans," *Wiley Journal on Wireless Communications and Mobile Computing*, August 2004.

[6] DAPAR, http://www.darpa.mil/ato/programs/WolfPack/index.htm.

[7] J. Bellardo and S. Savage, "802.11 denial-of-service attacks: Real vulnerabilities and practical solutions," in *In Proceedings of USENIX Security Symposium*, August 2003.

[8] X. Geng, Y. Huang, and A. B. Whinston, "Defending wireless infrastructure against the challenge of ddos attacks," *Mobile Networks and Applications*, vol. 7, 2002.

[9] M. K. Simon, J. K. Omura, R. A. Scholtz, and B. K. Levitt, *Spread Spectrum Communications Handbook*. McGraw-Hill, 2001.

[10] X. Liu, G. Noubir, R. Sundaram, and S. Tan, "Spread: Foiling smart jammers using multi-layer agility," in *Proceedings of the IEEE INFOCOM07 Mini-Symposium*, 2007.

[11] W. Xu, W. Trappe, Y. Zhang, and T. Wood, "The feasibility of launching and detecting jamming attacks in wireless networks," in *Proceedings of the ACM MOBIHOC05*, 2005.

[12] G. Noubir, "Collision-free one-way communication using reed-solomon codes," in *Proceedings of IEEE ISITA*, 1998.

[13] S. Lin and D. J. Costello, *Error Control Coding: Fundamentals and Applications*. Prentice-Hall, 1983.

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