**Table 1: Details of Simulation Scenarios**

| Parameter | SC1 | SC2 | SC3 | SC4 |
|---|---|---|---|---|
| Number of users ($N$) | 25 | 35 | 50 | 15 |
| Size of the covert set ($\|S\|$) | 16 | 21 | 33 | 10 |
| Covert transmitter min window size ($T_0$) | 4 | 7 | 8 | 4 |
| Expansion postpone parameter ($\alpha$) | 1 | 1 | 1 | 1 |
| Regular user min window size ($W_{min}$) | 16 | 32 | 32 | 16 |
| Number of back off stages ($M$) | 6 | 5 | 5 | 6 |

**Table 2: Security Tests for Different Scenarios**

| Scenario | KS-test | Regularity Score (Covert Transmitter) | Regularity Score (Regular Transmitter) |
|---|---|---|---|
| SC 1 | 0.0432 | 0.2704 | 0.2757 |
| SC 2 | 0.0398 | 0.2322 | 0.2509 |
| SC 3 | 0.0367 | 0.3772 | 0.3794 |
| SC 4 | 0.0353 | 0.2327 | 0.2534 |

are equipped with proper error correction methods in case a mismatch happens between the transmitter and the receiver.

Each covert message (i.e., $\omega$) is associated to a *unique state* in the first stage of the transmitter's transmission window (i.e., stage 0). The covert communication begins as the transmitter moves to the corresponding state of the covert message. Then, the transmitter monitors the channel to catch packets from members of the covert set. For each packet, the transmitter's clock is incremented by one unit and it moves down one state in its transmission window (to the left in Figure 1). The transmitter sends its next packet when it reaches the last state of the transmission window.

The receiver also maintains its covert clock similar to the transmitter. Hence, upon receiving a packet from the transmitter, the receiver reads the value of its clock, decodes the covert message, and resets the clock for the next message.

However, if the transmitter fails to transmit the packet on the proper time slot (e.g., due to collision), it expands its contention window and selects a new time slot that corresponds to the covert message. Indeed, this window expansion plays a critical role to maximize the stealthiness of the covert transmitter as it mimics the behavior of an ordinary CSMA node to handle collisions in the network. Thus,

$$T_i = \begin{cases} T_0 & 0 \leq i \leq \alpha \\ 2 \times T_{i-1} & \alpha < i \leq M \\ T_M & i > M \end{cases} \quad (1)$$

Where, $T_i$ is the size of the transmitter's contention window in the $i^{th}$ stage, and $M$ is the number of backoff stages. The parameter $\alpha$, is a design parameter that controls how far the transmitter deviates from behaviors of a regular user.

Finally, in order to keep synchronization between the transmitter and the receiver, following each unsuccessful packet transmission attempt, the transmitter waits for $T_i - \omega$ extra clock ticks (i.e., packets from members of the covert set) before moving to the next stage. Hence, at the beginning of the $i^{th}$ stage, the covert clocks at the receiver and the transmitter would be equal to $\sum_{j=0}^{i-1} T_j$, regardless of the covert message. The receiver removes this offset from its covert clock (i.e., $C_r$) and decodes the message as: $\omega = C_r \ mod \ T_0$.

## 3. PERFORMANCE ANALYSIS RESULTS

The performance analysis is performed on four scenarios (Table 1) using a CSMA testbed with Slot time $= 20\mu s$, SIFS $= 10\mu s$, DIFS $= 50\mu s$, Payload $= 1.5KB$, and Channel overt rate $= 1Mbps$.

In order to evaluate the stealthiness of the channel, we use the *Kolmogorov-Smirnov test* (KS-test) [5] and the *regularity test* [6]. The KS-test shows the difference between the distributions of the inter-packet delays sampled from the covert transmitter's traffic and the traffic originated from a regular node. The regularity test is designed to detect the abnormal behavior of the covert transmitter in reacting to the network events (e.g., packet loss). The test results in Table 2 verifies that the transmitter has similar long-term characteristics (KS-test) and short-term behaviors (regularity test) as compared to a regular CSMA node.

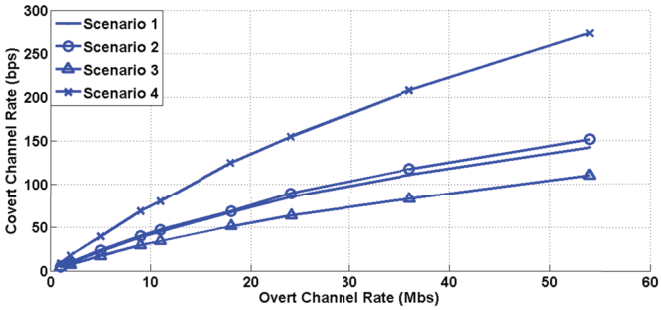


**Figure 2: Covert rate of the proposed channel.**

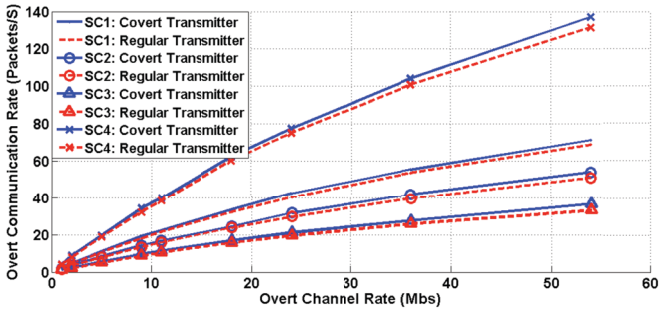


**Figure 3: Overt rate of the covert transmitter**

Figure 2 shows the achievable rate of the proposed covert channel. It is noted that the covert channel rate increases linearly with the capacity of the overt channel. The overt communication rate of the covert transmitter and regular users in the system are depicted in Figure 3. From the graph, it can be observed that the transmitter conveys the same overt rate as compared to regular users of the system. Thus, it is extremely difficult for a system observer to track the transmitter based on overt communication rate.

## 4. REFERENCES


[1] R. Kemmerer. Shared resource matrix methodology: An approach to identifying storage and timing channels. *ACM Trans. on Computer Systems*, 1(3):277, 1983.

[2] S. Bhadra, S. Bodas, S. Shakkottai, and S. Vishwanath. Communication Through Jamming Over a Slotted ALOHA Channel. *IEEE Trans. on Information Theory*, pages 54(11):5257, 2008.

[3] S. Li and A. Ephremides. A covert channel in MAC protocols based on splitting algorithms. In *IEEE WCNC*, pages 1168-1173, 2005.

[4] Z. Wang, J. Deng, R. Lee, and P. Princeton. Mutual anonymous communications: a new covert channel based on splitting tree MAC. In *IEEE INFOCOM*, pages 2531-2535, 2007.

[5] Y. Liu, D. Ghosal, F. Armknecht, A. Sadeghi, S. Schulz, and S. Katzenbeisser. Hide and Seek in Time: Robust Covert Timing Channels. *In ESORICS*, pages 120-135, 2010.

[6] S. Cabuk, C. Brodley, and C. Shields. IP covert timing channels: design and detection. In *ACM CCS*, pages 178–187, 2004.