Molecular Secure Channel

International Conference on ICT Convergence (ICTC 2017)

Secure Channel for Molecular Communications

Authors
S. M. Riazul Islam and Hyeonjoon Moon (Sejong University)
Farman Ali and Kyung-Sup Kwak (Inha University)

Date: October 18, 2017
Contents

- Introduction
- System Model
- Proposed Secure Channel
  - Secret Key Exchange Algorithm
  - Secured Molecular System
  - Energy Consumption Analysis
  - Simulation Performance
- Concluding Remarks
Introduction

- Molecular communication is promising to provide appropriate solutions for a wide range of applications including biomedical, industry, and environmental areas.

- Introducing security into molecular communications is a fundamental challenge for researchers. There exist very few works that focus on security aspects.

- In this article, we deal with eavesdropping, a special class of threats, that might exploit vulnerabilities to breach security in molecular communications.

- Secure Channel (Private Key Exchange for Data Encryption) is a common technique in conventional data communications for defending against eavesdropping.

- In this paper, we introduce secure channel for molecular communications.
System Model

Assumptions

- Time-slotted with specific slot duration.

- Communicating nanomachines are perfectly synchronized in time and number of molecules

- Symbols transmitted upon on-off keying (OOK) modulation

- Full-duplex system; nanomachines can transmit and receive at the same time

- Malicious nanomachine attempts to receive the transmitted molecules with the purpose of eavesdropping

- Both nanomachines use same type of molecules.
- Green molecules sent by nanomachine C, whereas violet molecules sent by A
Secret Key Exchange (1/2)

Diagram showing Nano Machine A, Nano Machine C, Resultant Molecules, and Information Bit Index.
Secret Key Exchange (2/2)

- Cases: Both machines transmit a zero (or one). The sum signal is zero (or double). But, this doesn’t help malicious machine B understands any bit of the secret key.

- Cases: Nanomachine A sends a one whereas nanomachine C sends a zero or vice versa. Both nanomachines can find what the other machine has transmitted, since they are aware of what information they themselves have just sent. Conversely, the malicious node B only understands the sum of two molecular signals and it cannot find out which machine sent the one and which machine sent the zero.

- Both machines accept all bits, where they transmitted different number of molecules. Now, they can consider either the bits transmitted by machine A or the bits transmitted by machine C as the secret key.

- Suppose a security scheme selects the nanomachine C for this purpose, the encryption key will be 0101. However, if the machine A is selected, the key is 1010.

- The key we have just obtained is 4-bits in length. Note that a secret key of any desired length can be achieved if both machines continue their operations until the target number of bits are stored.

- Algorithm is given in next slide.
Algorithm for Secret Key Exchange

1. Initialize Security Services
2. Invoke Synchronization
3. Symbol Timer Reset
4. Send a One or Zero Randomly
5. Check Symbol Timer
   - Symbol timer reaches preset time?
     - Yes: Detect molecules to receive the bit sent by other machine
     - No: Discard the present bit
6. Are sending and receiving bits same?
   - Yes: Store the present bit sent by predefined machine as a bit of secret key
   - No: Return the stored bits
7. Number of bits stored equals the desired length of the key?
   - Yes: Return the stored bits
   - No: Repeat from step 3
Secured Molecular System

Proposed Secure Channel: System
Energy Consumption Analysis

- $E_b^T$ and $E_b^C$ be the energy required to transmit one bit of information, and energy required to compute one bit of information, respectively.
- $N$: total number of information bits to be transmitted
- $K$: key length in bits.
- $M$: the number of key generation to complete the information transmission

The total energy required to transmit the information with security becomes

$$E_T^S = (1.002N + 2KM)E_b^T$$

In case of no security, the total energy required to transmit

$$E_T^0 = \text{Energy for Information Transmission} = N \times E_b^T$$
Performance Evaluation (Energy Consumption)

![Graph showing energy consumption for different security options.

- Usual transmission energy (theory)
- Additional energy for security (theory)
- Usual transmission energy (simulation)
- Additional energy for security (simulation)

Security options:
- No security
- 8-bit key
- 16-bit key
- 32-bit key
- 64-bit key

Energy consumption graph for simple hide operations and frequent changes of key.}
Concluding Remarks

- In this article, we have proposed a secured molecular communication system to defend against eavesdropping.

- The participating nanomachines exchange a secret key through molecular signaling in such a way that adversary cannot understand the key.

- This key exchange mechanism doesn’t require significant additional energy. Also, the use of XOR ciphering to encrypt and decrypt the data using the generated secret key make the system simple and effective in terms of energy consumption.

- The proposed system can effectively be used in molecular communication systems where simple hide operations are sufficient or more stringent security are required.
Discussion