Tsinghua Science and Technology

Volume 23 | Issue 2 Article 2

2018

Lightweight Trusted Security for Emergency Communication Networks of Small Groups

Fugang Liu
the Department of Electronics and Information and Engineering, Heilongjiang University of Science and Technology, Harbin 150022, China.

Jiawei Xu
Shanghai University, Shanghai 200000, China.

Feng Hu
Shanghai University, Shanghai 200000, China.

Chao Wang
Shanghai University, Shanghai 200000, China.

Jie Wu
the Department of Computer and Information Sciences, Temple University, Philadelphia, PA 19122, USA.

TSINGHUA SCIENCE AND TECHNOLOGY
ISSN 1007-0214 04/09 pp195–202
DOI: 10.26599 / TST.2018.9010032
Volume 23, Number 2, April 2018

Lightweight Trusted Security for Emergency Communication Networks of Small Groups

Fugang Liu, Jiawei Xu, Feng Hu, Chao Wang*, and Jie Wu

Abstract: Public communication infrastructures are susceptible to disasters. Thus, the Emergency Communication Networks (ECNs) of small groups are necessary to maintain real-time communication during disasters. Given that ECNs are self-built by users, the unavailability of infrastructures and the openness of wireless channels render them insecure. ECN security, however, is a rarely studied issue despite of its importance. Here, we propose a security scheme for the ECNs of small groups. Our scheme is based on the optimized Byzantine Generals' Problem combined with the analysis of trusted security problems in ECNs. Applying the Byzantine Generals' Problem to ECNs is a novel approach to realize two new functions, debugging and error correction, for ensuring system consistency and accuracy. Given the limitation of terminal devices, the lightweight fast ECDSA algorithm is introduced to guarantee the integrity and security of communication and the efficiency of the network. We implement a simulation to verify the feasibility of the algorithm after theoretical optimization.

Key words: emergency communication networks of small groups; optimized Byzantine Generals' Problem; fast ECDSA; lightweight trusted security scheme based on Byzantine Generals' Problem

1 Introduction

The establishment of a reliable, fast, safe, and effective emergency communications system is necessary for the government to develop disaster relief management plan[1−3]. The analysis of data from a group of 64 students who experienced the 2015 stampede in the Bund revealed that signals were unavailable for most people at the time of the incident[4−6]. Therefore, data channels and circuit channels failed to work, thus causing a break down in the flow of information and causing the accident to deteriorate further. Similarly, many emergency situations occurring in daily life require reliable and safe communication networks to enable survivors to call for help and for rescuers to analyze and propose the most efficient rescue plan. Thus, the emergency communication network systems are greatly important to our daily lives.

Currently available emergency communication systems rely on shortwave and satellite communications, which both require special technology and equipment that only some special units, such as government units, militaries, and telecommunications companies, can access. Therefore, research on mobile terminals with Bluetooth or Wi-Fi communication has developed in recent years. These terminals play important roles in emergency situations. For example, Fire Chat allows users to send information to anyone within 30 meters through the use of wireless signals or Bluetooth devices. Moreover, it can take another user's phone as a springboard to extend communication distance. The Lion Company, a subsidiary of Apple Corp, has proposed Air-Drop, a novel feature,

• Fugang Liu is with the Department of Electronics and Information and Engineering, Heilongjiang University of Science and Technology, Harbin 150022, China. E-mail: liufugang_36@163.com.
• Jiawei Xu, Feng Hu, and Chao Wang are with Shanghai University, Shanghai 200000, China. E-mail: wangchao@staff.shu.edu.cn.
• Jie Wu is with the Department of Computer and Information Sciences, Temple University, Philadelphia, PA 19122, USA. E-mail: jiewu@temple.edu.
* To whom correspondence should be addressed.
Manuscript received: 2017-07-22; accepted: 2017-11-21

that utilizes direct Wi-Fi technology to share files between multiple devices separated by a distance of 30 feet.

In recent years, many researchers have devoted themselves to the study of Emergency Communication Networks (ECNs). Zhao and Wu[7] proposed a human network driven by the information sharing system B-SUB. The introduction of the Temporal Counting Bloom Filter (TCFB) enables the encoding of contents and human interest as tags in the system to reduce terminal consumption and realize further real-world trace-driven simulations that ensure the efficiency of B-SUB under different network conditions[7]. Gomez et al.[8] proposed the ABSOLUTE project and focused on designing, prototyping, and demonstrating a high-capacity IP mobile data network with low latency and extensive suitable for many forms of multimedia delivery in different settings, including public safety scenarios. Markakis et al.[9] presented the EMYNOS project, for the design and implementation of a next-generation platform capable of accommodating rich-media emergency calls that combine voice, text, and video, thus providing a powerful tool for coordinating communication among citizens, call centers, and first responders.

However, previous groups have mainly focused on the establishment, efficiency, and availability of ECNs, whereas few have focused on the security problem encountered by ECNs. Although, the Byzantine Generals' Problem is a hot security problem[10], it has seldom been applied to emergency networks. The existence of malicious nodes, called Byzantine fault nodes, may lead to software errors, operation faults, and malicious attacks. For example, in the case of a fire emergency, wrong instructions caused by malicious nodes may have severe consequences. Compared with the original Byzantine Generals' Problem, real-life emergency situations are more complex, and anyone may act as a malicious node that can release incorrect information that then affects the whole network. Thus, error correction and debugging are crucial for ECNs in real-life application. However, error correction and debugging are unavailable for known algorithms encountering the Byzantine Generals' Problem. In addition, these algorithms have other objective limitations, such as the the power consumption and computing abilities of their terminal devices.

To solve the above problems, this study proposes an optimization approach for the Byzantine Generals' Problem. The proposed approach is combined with the lightweight fast ECDSA algorithm to provide a safe and efficient environment for ECNs. The system realizes the new functions of error correction and debugging and guarantees the consistency and accuracy of the system. The feasibility of error correction and debugging is successfully verified through a simulation of the scheme.

2 Byzantine Generals' Problem

2.1 Traditional Byzantine Generals' Problem

The original Byzantine army problems derived from a military problem encountered during the period of the Byzantine Empire. This problem supposes that several Byzantine armies have settled outside of an enemy's town. Each division has an adjutant who could communicate with other adjutants only through messengers. Assume that some adjutants are traitors that will deliberately deliver incorrect messages to other adjutants. If the number of the traitors is too large, the general cannot effectively identified the traitors. The Byzantine Generals' Problem has three conditions[10]:

Condition 1 No solutions exist if more than 1/3 of the soldiers have betrayed their positions.

Condition 2 The Oral Message (OM) algorithm is deployed as a solution if the proportion of traitorous soldiers is less than 1/3 of the total number of soldiers.

Condition 3 The signed message algorithm could be deployed as a solution if more than 2/3 of the total number of soldiers is loyal.

The OM algorithm should meet the following assumptions:

Assumption 1 All information sent out will be received by the corresponding receiver.

Assumption 2 Every receiver knows who sent the message.

Assumption 3 Missing information can be detected.

Assumptions 1 and 2 prevent traitors from interfering with communication between two other adjutants, and Assumption 2 guarantees that the message cannot be modified. Assumption 3 prevents traitors from trying to affect results without forwarding a message. The OM algorithm follows the two conditions;

Condition 1 Algorithm OM(0):

(1) The general sends commands to adjutants;

(2) Every adjutant acts upon the order.

Condition 2 Algorithm OM$(m): m > 0$:

(1) The general sends commands to adjutants;

(2) All adjutants save the message and continue to run OM$(m-1)$, that is to say, adjutant i will send V_i to the other $n-2$ adjutants.

(3) All adjutants receive $n-1$ messages, and every adjutant

executes the command in accordance with the principle of majority rule (if the number of attacks is as many as that of retreats, the default command is retreat).

For the traditional Byzantine general problem, if the number of traitors is m and the number of solders is greater than $3m+1$, the algorithm can ensure consistency and correctness. Debugging and error correction should be realized before OM can be applied to the ECNs of small groups.

2.2 Optimized OM algorithm

As in the ECNs of small groups, our concerns not only center on identifying whether everyone has reached a consensus but also on identifying malicious nodes that should be removed from the network. Therefore, an optimized OM algorithm with debugging and error correction functions should be considered.

As detailed above, we should first suppose that the number of traitors is less than 1/3 of the population. The optimized OM algorithm is described as follows:

(1) The general sends commands to adjutants.

(2) Every adjutant i sends V_i from the general to the other $n-2$ adjutants.

(3) Every adjutant i exchanges messages from other $j\,(j \neq i)$ adjutants (received in step 2). That is, every adjutant i asks another $j\,(j \neq i)$ adjutant what they received from other adjutants.

(4) Every adjutant i horizontally compares messages received in step 3. If the number of received commands different from other commands is greater than $(n-1)/3$, then the nodes sent different messages. Therefore, the adjutants are traitors and should be removed.

(5) After all traitors are removed, all loyal adjutants exchange commands from the generals. If the commands sent by the general are inconsistent, then the general is a traitor, and the armies should not obey the order. Debugging and error correction are thus achieved.

Take $m=2, n=7$ as an example, in which two traitors are present among seven adjutants (shown in Fig. 1).

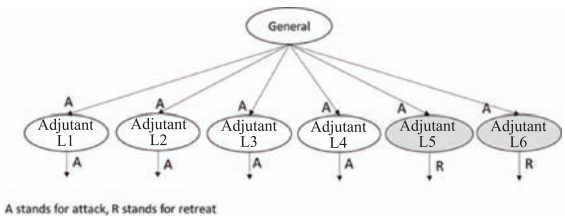

Fig. 1 L5 and L6 are traitors.

First, the general sends attack commands to all adjutants. After the adjutants receive their commands, L1−L4 will forward the original attack command A to other adjutants as L5 and L6 begin to lie and send tampering commands to other adjutants. Then, the adjutants will exchange commands received from other adjutants during the last round. Taking L1 as an example (Table 1). Table 1 shows that adjutants Li (i=2-6) respectively exchange what they have received from other adjutants with L1.

Only L5 and L6's answers are different from the other adjutants' answers. Thus, L5 and L6 are traitors and should be removed. Debugging and error correction are realized through the above steps.

The condition that the general is a traitor is shown in Fig. 2.

When the general is a traitor, he will send different commands to the adjutants to confuse the public. After all adjutants have received the command, the adjutants make the second exchange; taking L1 as an example (Table 2).

Table 1 Messages received from others (L5 and L6 are traitors).

	L1=A	L2	L3	L4	L5	L6
L1	L2	A	A	A	X	X
	L3	A	A	A	Y	Y
	L4	A	A	A	Z	Z
	L5	X	X	X	W	W
	L6	Y	Y	Y	U	U

Note: A stands for attack; X, Y, Z, W, and U stand for unknown information. For example, L2 Row shows commands sent to L1 by L2, and the commands are exchanged between L2 and other adjutants.

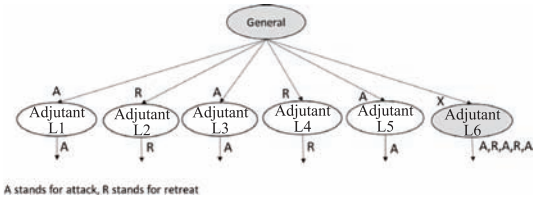

Fig. 2 The general and L6 are traitors.

Table 2 Messages received from others (the general and L6 are traitors).

	L1=A	L2	L3	L4	L5	L6
L1	L2	R	R	R	R	X
	L3	A	A	A	A	Y
	L4	R	R	R	R	Z
	L5	A	A	A	A	W
	L6	A	R	A	R	U

Note: A stands for attack; R stands for retreat; and X, Y, Z, W, and U stand for unknown information.

The message sent by L6 are always different from those sent by others. Therefore, L6 must be a traitor, and the command sent by L6 should be ignored. Then L1 will ask other nodes what commands they received during the first round (Table 3).

As seen in Table 3, the general lies. Thus, the general is a traitor and should be removed from the network. The above section provides an outline of the whole process of the optimized OM algorithm which ensures correctness, consistency, and debugging.

3 Fast ECDSA

As stated in Section 1, although the terminal device of ECNs cannot offer powerful calculation capability, the efficiency and security of the network should be guaranteed. Specifically, we need a safe and efficient algorithm for communication. The efficiency of fast ECDSA is superior to that of ECDSA given that the former adopts binary shift NAF codes for scalar multiplication[11]. In this case, the fast ECDSA for securing the routing scheme is as follows:

Step 1: Set an elliptic curve domain parameter $D = (F, a, b, p)$, where F is the finite field GF(p^n), $a, b \in \mathrm{GF}(p^n)$, G is the base point, and $\#\mathrm{E}(\mathrm{GF}(p^n))$ is the order of the elliptic curve.

Step 2: Fast ECDSA signature generation is described as follows:

(1) Select the secret random integer k, $k_A \in [1, n-1]$.

(2) Compute $kG = (x_1, y_1)$ (where y_1 is not needed for computation) and $r = x_1 \bmod p_1^n$, if $r = 0$, then return (1) and reselect k.

(3) Compute $k^{-1} \bmod p_1^n$.

(4) Compute $e = MD5(m)$.

(5) Compute $s = k^{-1}(e + k_A r) \bmod p_1^n$, if $s = 0$, then return (1) and reselect k.

(6) Fast ECDSA signature of message m, namely the integers (r, s), then A sends $(m||r||s||k_A)$ to B.

Step 3: Signature verification is described as follows:

(1) When B receives the signature, verify that r, s are integers in the interval $[1, n-1]$. If any verification fails, directly reject the signature.

(2) B computes $e = MD5(m)$ and $w = s^{-1} \bmod p_1^n$.

(3) B computes $u_1 = ew \bmod p_1^n$ and $u_2 = rw \bmod p_1^n$.

(4) B computes $a = (u_1 + u_2 \times k_A) \bmod p_1^n$.

Table 3 Messages received in the first round.

L1	L2	L3	L4	L5	L6
A	R	A	R	A	X

(5) B computes the multiplication point of $a \times G = x_1'$ in the Montgomery curve.

(6) B computes $v = x_1' \bmod p_1^n$.

(7) If $r = v$, then accept the signature of A.

The algorithm uses the Montgomery elliptic curve, which can effectively resist time and energy attacks. Meanwhile, the calculation speed of the Montgomery elliptic curve is faster than that of the traditional Weierstrass elliptic curve. Simulation results[10] have shown that fast ECDSA can reduce the time ratio of signature generation and verification from 2 to 1.2 with a reduction of approximately 40%. Therefore, signature generation and verification can be conducted on mobile terminals with limited power and energy consumptions. Fast ECDSA is thus a viable candidate for ECNs.

4 Design and Simulation of a Lightweight, Secure Routing Scheme Based on the Byzantine Generals' Problem

This study introduces a lightweight, secure routing scheme for protecting the ECNs of small groups from malicious nodes. The scheme is based on the Byzantine Generals' Problem. We explore the feasibility of combining the optimized OM algorithm for the Byzantine Generals Problem to ensure the security of ECNs in small groups with content-based routing and interest tags to select the route for information transfer. Then, we adopt the fast ECDSA during route selection and data transfer to ensure data integrity and security. After data transmission, the optimized OM algorithm is used to remove malicious nodes from networks, thus achieving debugging and error correction. Our algorithm is simple, effective, and requires low computational complexity and storage overhead while providing high security. Figure 3 shows the whole process of the algorithm:

Step 1: Initialize every node's interest tag and use the Hash function to convert them to a fixed length interest abstract.

Step 2: Match the interest abstracts of routing information with one another.

Step 3: Use fast ECDSA for signature verification on the corresponding data to ensure the security and integrity of data.

Step 4: After data transmission, use the optimized Byzantine Generals' protocols to remove malicious nodes to prevent attacks and realize debugging and error correction.

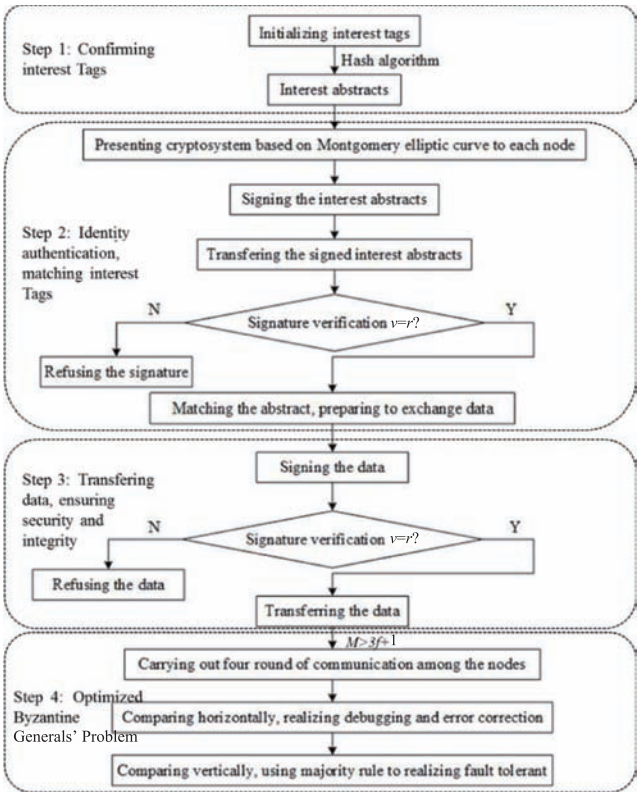

Fig. 3 Flow diagram of lightweight, secure routing scheme based on Byzantine Generals Problem.

4.1 Signature and verification

When the scope of the ECNs is determined, the head node will issue each node an encryption system certificate based on the Montgomery elliptic curve.

The key part is to select a suitable and safe Montgomery elliptic curve. First, we should select an elliptic curve order within a certain range. A prime factor of more than 1014 in orders indicates a valid curve. Every node uses fast ECDSA for signature and verification, and if verification is passed, the node will receive the message.

Mobile phone-processors with frequencies of more than 1 GHz need approximately 9.6×10^{-4} seconds to solve the ECC algorithm. Memory sizes for encryption and decryption processes are 2180 and 2240 bytes, respectively. These requirements could be easily met by currently available mobile phones with memories greater than 1 GB. The lightweight ECC algorithm further shows three advantages in the following aspects:

(1) Low computation complexity.

(2) A combined public key system ideology is adopted to reduce storage overhead.

(3) The combined public key system ensures system safety and prevents system decryption with a public key.

4.2 Node-level optimized Byzantine Generals' Problem

If N nodes and f Byzantine fault nodes exist in the network that meets $3f + 1 \leqslant N$, running the optimized OM algorithm among the nodes can successfully realize fault tolerance, debugging, and error correction after four rounds of communications. These effects will eventually eliminate the influence of Byzantine fault nodes and remove nodes from the network, as shown in Fig. 4:

(1) In the first round, the send node will send messages to all receiving nodes.

(2) In the second round, all receiving nodes will exchange the received messages, and normal nodes will forward the message honestly, whereas malicious ones will lie.

(3) In the third round, every receiving node will ask every other receiving node what it received during the second round. Then, they compare messages horizontally and vertically. Finally, the malicious receiving node is removed, and its messages are ignored.

(4) In the fourth round, all normal receiving nodes exchange their messages from the send nodes and judge whether the send node is normal, finally, realizing the function of debugging.

If the traffic denotes the number of data packets transmitted in the communication from a certain node request, the debugging will need four rounds of communications to take the optimized Byzantine Generals' Problem. The traffic is $N^3 + 3N^2 + 3N - 2 - 3f - 2Nf + f^2$.

4.3 Load-level selected trusted routing

The load level adds an authentication factor and interest tags to help find the trusted route rapidly.

(1) Interest tags

In content-based routing, every node has a TCBF that stores its interest tags and others' interest tags with a fixed length after conversion by a specific Hash algorithm. Such an approach hinders tag modification. Zhao and

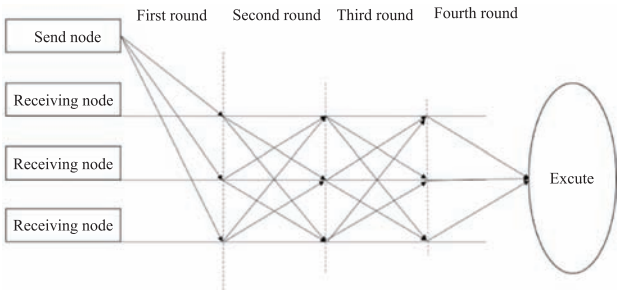

Fig. 4 Node-level optimized Byzantine Generals' Problem.

Wu[7] indicated that 86% of user-selected titles will be consistent. Thus, using tags on behalf of the users' interests is convenient and safe. When two nodes meet, whether or not the data packet should be transmitted can be determined by matching TCBF.

(2) Authentication factors

Each TCBF of the node will carry the public key information of the previous one, thus contributing to the certification of the security and reliability of the last node and guaranteeing the integrity of the routing information.

4.4 Simulation based on the above scheme

This study performed a simulation of 26-node ECNs of small groups to verify the feasibility of the optimized Byzantine Generals' Problem and test whether the system can realize debugging. The environment is as follows:

CPU: Intel-i54200M;

RAM: 12 GB;

SOFTWARE: OPNET Modeler Release 14.5;

NETWORK RANGE: $100\ \mathrm{m} \times 100\ \mathrm{m}$.

To analyze the debugging function intuitively, we first give the transmission rate of data packets without any malicious nodes as shown in Fig. 5. The transmission rate of data packets remains constant to some extent, indicating that the system is safe and satisfying the consistency without any malicious nodes.

Then, we introduce six malicious nodes as shown in Fig. 6. In this figure, malicious nodes are circled in red. Again, a precondition of the Byzantine Generals' Problem is that the number of malicious nodes must be no more than 1/3 of the total number of nodes.

The whole network includes three types of nodes: (1) Common nodes (mobile_node_1—mobile_node_26): These nodes include malicious nodes, head, and normal nodes. (2) Control node (node 3): This node controls the transmitting distance of the wireless signal of each node in

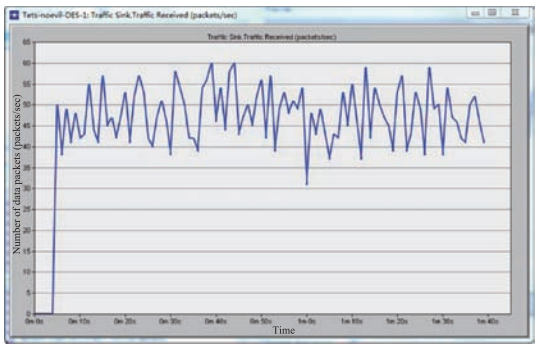

Fig. 5 Transmission rate of data packets without any malicious nodes.

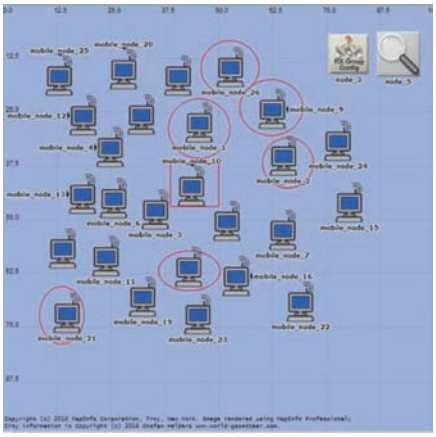

Fig. 6 26-node ECNs of a small group. Malicious nodes are circled in red, and the total node is marked by a square.

the network. (3) Configuration node (node 5): This node is responsible for configurations, such as node initialization. It can also check the network and distribute mac_id for each node in the network. If the number of malicious nodes exceeds 1/3 of the total number of nodes, the system should be initialized again.

Figure 7 shows one function of the configuration node (encircled in red) in which the system will break down as a result of the optimized Byzantine Generals' Problem under the condition that the number of malicious nodes is more than 1/3 of the total number.

Security schemes state that all normal nodes in the system can identify malicious nodes. As shown in Fig. 8,

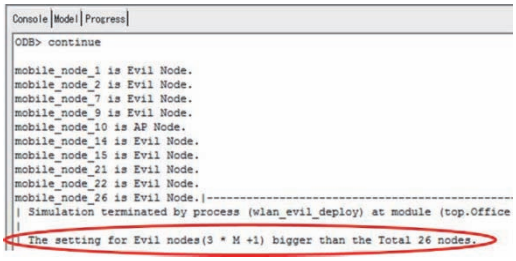

Fig. 7 The number of malicious nodes must be more than 1/3 of the total number of nodes.

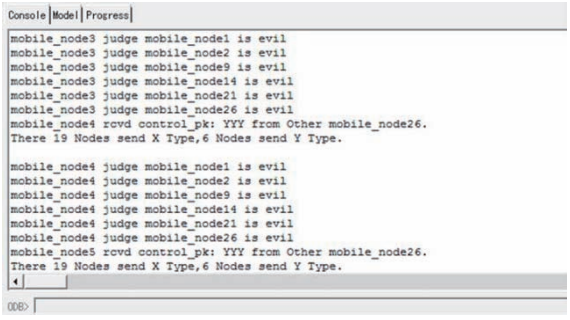

Fig. 8 All normal nodes in the network can identify malicious nodes.

the system prints out all the malicious nodes. This action corresponds to the initialization.

When the malicious nodes are identified, all normal nodes would actively disconnect (after 50 seconds) from these nodes. Then the number of transmission data packets in the network decreases (Fig. 9).

By combining the original safe network shown in Fig. 8 and the unsafe network with the 6 malicious nodes shown in Fig. 9 into Fig. 10, we find that all normal nodes that disconnect from identified malicious nodes show a sharp flow of data packets. This result indicates that the optimized Byzantine Generals' Problem effectively identifies malicious nodes and removes them while maintaining real-time communication. Additionally, in real application, the range of the optimized Byzantine Generals' algorithm mainly depends on the power of the user's device.

5 Conclusion

This study proposed an optimized OM algorithm for the Byzantine Generals' Problem to solve the security problem of ECNs. The algorithm is combined with content-based routing and fast ECDSA to yield a lightweight, trusted security scheme that realizes two new functions, debugging and error correction. A principle-of-proof simulation revealed that the scheme can enable secure data transmission in ECNs and debug and correct errors. Compared with other approaches, the scheme requires lower computational complexity and storage overhead while providing superior security. These characteristics meet the requirements such as limited power consumption and computation capability of mobile terminals.

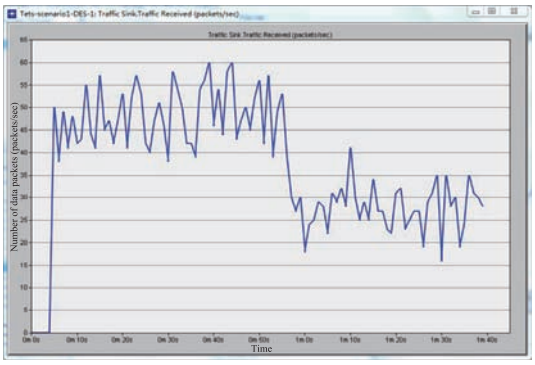

Fig. 9 Transmission rate of data packets in the system with 6 malicious nodes.

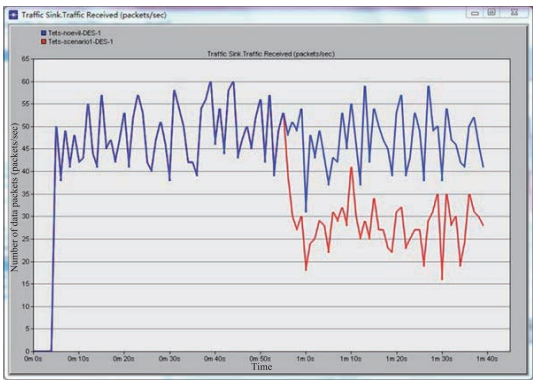

Fig. 10 Comparison of the transmission rate of data packets.

References

[1] F. Hu, C. Wang, H. G. Zhang, and J. Wu, Simple method for realizing Weil theorem in secure ECC generation, *Tsinghua Sci. Technol.*, vol. 22, no. 5, pp. 511–519, 2017.

[2] C. Wang, F. Hu, H. G. Zhang, and J. Wu, Evolutionary cryptography theory-based generating method for secure ECs, *Tsinghua Sci. Technol.*, vol. 22, no. 5, pp. 499–510, 2017.

[3] R. Grodi and D. B. Rawat, UAV-assisted broadband network for emergency and public safety communications, in *Proc. 2015 IEEE Global Conf. Signal and Information Processing*, Orlando, FL, USA, 2015, pp. 10–14.

[4] J. B. Wang, Y. L. Wu, N. Yen. S. Guo, and Z. X. Cheng, Big data analytics for emergency communication networks: A survey, *IEEE Commun. Surv. Tut.*, vol. 18, no. 3, pp. 1758–1778, 2016.

[5] A. Bhatnagar, A. Kumar, R. K. Ghosh, and R. K. Shyamasundar, A framework of community inspired distributed message dissemination and emergency alert response system over smart phones, in *Proc. 8^{th} Int. Conf. Communication Systems and Networks*, Bangalore, India, 2016, pp. 1–8.

[6] M. Raza, H. Le-Minh, N. Aslam, S. Hussain, and W. Ellahi, A control channel based MAC protocol for time critical and emergency communications in industrial wireless sensor networks, in *Proc. 2017 Int. Conf. Communication, Computing and Digital Systems*, Islamabad, Pakistan, 2017, pp. 122–126.

[7] X. Y. Zhao and J. Wu, The design and evaluation of an information sharing system for human networks, *IEEE Trans. Parallel Distrib. Syst.*, vol. 25, no. 3, pp. 796–805, 2014.

[8] K. Gomez, S. Kandeepan, M. M. Vidal, V. Boussemart, and R. Ramos, Aerial base stations with opportunistic links for next generation emergency communications, *IEEE Commun. Mag.*, vol. 54, no. 4, pp. 31–39, 2016.

[9] E. K. Markakis, A. Lykourgiotis, I. Politis, A. Dagiuklas, Y. Rebahi, and E. Pallis, EMYNOS: Next generation emergency communication, *IEEE Commun. Mag.*, vol. 55, no. 1, pp. 139–145, 2017.

[10] T. Clouqueur, K. K. Saluja, and P. Ramanathan, Fault

tolerance in collaborative sensor networks for target detection, *IEEE Trans. Comput.*, vol. 53, no. 3, pp. 320–333, 2004.

[11] C. Wang, X. Y. Shi, and Z. H. Zhu, The research of the promotion for ECDSA algorithm based on montgomery-form ECC, *J. Commun.*, vol. 31, no. 1, pp. 9–13, 2010.

Fugang Liu received the B.S. degree in computer science and technology from the Heilongjiang University of Science and Technology in 2004. He received the M.S. and Ph.D. degrees in communication and information system in 2009 and 2013, respectively, from Harbin Engineering University. He is currently an Assistant Professor with the Heilongjiang University of Science and Technology University. His research interests include DOA estimation of wideband signals, D-InSAR technique, and array signals processing. He is the author of three books, 12 articles, and 15 inventions, and was awarded Science and Technology Prize of Coal Industry Association of China in 2014.

Jiawei Xu is currently a master student in Shanghai University. Her research interest is information security. She received the bachelor degree in 2014 from Shanghai University of Electric Power.

Feng Hu received a B.S degree from the Xi'an University of Science and Technology. Currently, he is a PhD student at Electronic and Information Engineering Dept. of Shanghai University. His research interests include information security and quantum computing cryptography.

Chao Wang received the PhD degree from Tongji University in 1999. Currently, he is the IEEE Senior Member, Council Member of China Association of AI, the Information Security Committee Vice Chair of China Electronics Institute, Committeeman of the Sixth Shanghai Expert Committee for Informatization, Directorate of China artificial intelligence Institute, Committeeman of CCF, IEEE Shanghai Section Secretary, IEEE Shanghai CAS Chapter Vice Chair, and IEEE Shanghai Computer Chapter Vice Chair. His research interests include wireless sensor network, network information security and ECC, and quantum computing cryptography.

Jie Wu received the PhD degree from Florida Atlantic University in 1989. He is the chair and a Laura H. Carnell Professor in the Department of Computer and Information Sciences at Temple University. Prior to joining Temple University, USA, he was a program director at the National Science Foundation and a distinguished professor at Florida Atlantic University. His current research interests include mobile computing and wireless networks, routing protocols, cloud and green computing, network trust and security, and social network applications. He regularly published in scholarly journals, conference proceedings, and books. He serves on several editorial boards, including *IEEE Transactions on Computers, IEEE Transactions on Service Computing*, and *Journal of Parallel and Distributed Computing.*