Minimizing collaborative attacks in a real heterogeneous mobile ad hoc network using cooperative immunization model

Tao Gong[1, 2, *], Bharat Bhargava[2], Jiajia Zhou[1], Mehdi Azarmi[2], and Changxing Du[1]
[1] College of Information Science and Technology, Donghua University, Shanghai 201620, China
2 Department of Computer Science, Purdue University, West Lafayette, IN 47907, USA
CERIAS, Purdue University, 656 Oval Drive, West Lafayette, IN 47907-2086, USA

ARTICLE INFO
Article history:
Received
Received in revised form

Accepted

ABSTRACT
In this paper, a security problem of cooperative immunization against collaborative attacks such as the blackhole attacks and the wormhole attacks in a real heterogeneous mobile ad hoc network was discussed. Due to the vulnerabilities of the protocol suites, collaborative attacks in the mobile ad hoc network may cause more damages than individual attacks. In human immune system, non-selfs (i.e. viruses, bacteria and cancers etc.) often attack human body in a collaborative way, and cause diseases in the whole body. Inspired from the human immune system, we built a tri-tier cooperative immunization model to detect the collaborative attacks (non-selfs) and eliminate them in the real mobile ad hoc network. The threat model of the collaborative attacks was developed to analyze the vulnerabilities of the real heterogeneous mobile ad hoc network. Real experimental results and simulations demonstrate the validation and effectiveness of the proposed secure model in minimizing the collaborative attacks.

Keywords:
Cooperative immunization
Mobile Ad Hoc Networks
Security
Collaborative attacks
Non-selfs

1. Introduction

Security is a key challenge in the mobile ad hoc networks, since these networks use a suite of the shelf protocols, which makes all standard vulnerabilities of those protocols available to the attackers. The IEEE 802.11 is a set of standards for implementing wireless local area network (WLAN) computer communication in the 2.4, 3.6 and 5 GHz frequency bands. These standards provide the basis for wireless network products using the Wi-Fi brand name. IEEE 802.15.4-2003

* Corresponding author.
E-mail addresses: tgong@purdue.edu (T. Gong), bb@cs.purdue.edu (B. Bhargava)

(Low Rate WPAN) deals with low data rate but very long battery life (months or even years) and very low complexity. Several standardized and proprietary networks (or mesh) layer protocols run over 802.15.4-based networks, including IEEE 802.15.5, ZigBee, 6LoWPAN, and ISA100.11a. The IEEE 802.16 standard provides a high-speed broadband access (up to 40 Mbps) with large coverage, which makes it more flexible and usable in many scenarios than the other alternative technologies such as DSL or WiFi.

Recently, the availability of practical swarm intelligence and multi-agent algorithms can help attackers to collaborate and realize more effective attacks against defense mechanisms more effectively (Bhargava et al., 2009). Though the current mobile ad hoc networks use some individualized security approaches such as antivirus software (Sukwong et al., 2011), intrusion detection tools (Zhou et al., 2010), mail filtering applications (Garcia-Osorio et al., 2010) etc., these mobile ad hoc networks are not secure against the collaborative attacks because they are designed against only individual attacks.

Collaborative attacks are launched by some malicious adversaries that synchronize their activities to accomplish disruption, deception, usurpation, and disclosure against the targeted network entities (Bhargava et al., 2009). For instance, if the SYN flood attack and the slammer worm are launched in a coordinated way, the resulting consequences will be devastating and very difficult to deal with (Moore et al., 2003; Schuba et al., 1997). For instance, many attackers can influence the decision-making of some core machines with routing Sybil attacks (Douceur 2002).

In general, threat modeling is used to expose some circumstances or events having the potential to cause harm to a system in the form of destruction, disclosure, modification of data, and/or denial of service, and results in a vulnerability assessment (IEEE Std 1074- 2006, 2006). Similar to the threat model, the immune danger theory was proposed by Matzinger (2002), and in this danger theory immune response distinguishes the danger signals that are generated by damaged cells. In the real mobile ad hoc network of this paper, the threats are the damaged selfs, i.e. the compromised nodes, and the foreign non-selfs such as the blackhole attacks and the wormhole attacks, so the threats are the non-selfs in nature. The blackhole attacks can transmit malicious broadcast information from a node that the node has the shortest path to the destination aiming to intercept messages (Ramaswamy et al., 2005). The wormhole attacks can record packets at one location in the network, tunnel them to other locations, and retransmit them there into the network (Wang et al., 2006). The collaborative attacks of blackhole and wormhole almost have all the abilities of the two attacks, and the two attacks can enhance each other sometimes (Bhargava et al., 2009).

To deal with the collaborative attacks, some cooperative approaches have been designed and used on matching the features of multiple attacks in the collaborative way. But these approaches are often ineffective to unknown attacks (Sukwong et al., 2011). In fact, human immune network is a natural cooperative defense system against various collaborative attacks from viruses, bacteria and cancer etc. (Gong et al., 2011), and the biological network inspires us to design more advanced defense system against the collaborative attacks. Both RNA-containing and DNA-containing viruses, two obviously different classes of virus, can cause cancer (Robert 1965), and so bacteria with the viruses and cancer can cause the overload and damages of the immune system. In general, the human immune network has a large number of immune cells (e.g. B cells and T cells) and immune molecules (Bordon 2011). The first step for the immune network against the collaborative attacks is to detect and determine whether the objects are selfs (Gros1 2011). If

they are selfs, the objects are not attacks; otherwise, the objects are the non-selfs that cause attacks. The first mission of the native immune tier is to detect selfs and attacks. The other responsibilities of the tier are to recognize and classify known attacks. For unknown attacks, immune learning and memorization mechanisms are necessary for the immune network to decrease & control the attacks and these functions are deployed on the adaptive immune tier (Ziv1 et al., 2006).

A bio-inspired anti-worm static artificial immune system was proposed and evaluated based on the tri-tier immune model (Gong et al., 2006). The immune model was also used in software fault diagnosis of mobile robots (Gong et al., 2008). In this paper, a new cooperative immunization model against the collaborative attacks in the real heterogeneous mobile ad hoc network was proposed and evaluated. The immune model was used to detect and minimize the attacks. The cooperative immunization model was proposed against the collaborative attacks in the mobile ad hoc networks in section 3. In section 4, the detection & learning capabilities of the immunization model in a cooperative way was analyzed. In section 5, a simulation study of cooperative immune network against collaborative attacks was given. Section 6 concluded the paper.

2. Related work

The vulnerabilities of the mobile ad hoc networks have been analyzed in the literature. In the following the main characteristics of the vulnerabilities were reviewed briefly.

Bhargava et al. (2009) regarded some support to DES as an important vulnerability in WiMAX standards, because DES can be broken by collaborative attacks. Second, attacks in the IEEE 802.16j standard include blackhole attacks (Ramaswamy et al., 2005), wormhole attacks (Wang et al., 2006), denial- of-message (DoM) attacks (McCune et al., 2005) and sybil attacks (Yu et al., 2006) etc. Besides, the implementation bugs and the incompatibilities are also the potential sources of vulnerabilities (Bhargava et al., 2009).

To defend against the collaborative attacks, a few of cooperative approaches have been proposed recently. For example, Cheung et al. (2003) decomposed some cyber attacks into multiple sub- attacks and developed a method to model multistep attack scenarios based on typical isolated alerts about attack steps. Li et al. (2007) built a stochastic model of collaborative internal and external attacks. Yang et al. (2000) designed a signature-based model to detect collaborative attacks. Based on multicast, annotated topology information, and blind detection techniques, Hussain et al. (2003) built a collaborative system to detect distributed DoS (DDoS) attacks. Ourston et al. (2004) used Hidden Markov models to detect collaborative attacks. Cuppens et al. (2002) made each Intrusion Detection System (IDS) in collaborative IDSs send its triggered alerts to a central module, in order to reduce the number of false positives. The central module correlates the incoming alerts of all IDSs and generated a more elaborated and general alarm to the whole system. Lin et al. (2008) shared the information from the node that detected the intrusion to the other nodes, so that they can save time and energy for doing pattern matching which is a demanding task. Yu-Sung et al. (2003) proposed a collaborative intrusion detection system (CIDS) for different sorts of IDSs to work cooperatively.

To overcome the disadvantages of the IDS approaches against the unknown attacks, the techniques of immune computation have been investigated for some security applications. Dasgupta et al. (2002) presented a technique inspired by the negative selection mechanism of the immune system that can detect foreign patterns in the non-self space. Because malicious computer software in the form of viruses and worms continues to plague modern information networks,

Balthrop et al. (2004) surveyed the structure of computer networks and analyze their epidemiological characteristics. Esponda et al. (2002) proposed a formal framework to analyze the tradeoffs between positive and negative detection schemes in terms of the number of detectors needed to maximize coverage.

3. Cooperative immunization model against collaborative attacks

Based on the tri-tier immune model as shown in Fig. 1, a real mobile ad hoc network was immunized for security, as shown in Fig. 2.

Fig. 1 - Tri-tier cooperative immunization. The three tiers of immune model include native immune tier, adaptive immune tier and network tier.

Fig. 2 – A real mobile ad hoc network.

The native immune tier is used to detect attacks in a cooperative way, and the self is the most important factor in increasing the efficiency and effectiveness of the attack detection process. The second tier is adaptive immune tier that is used to learn and recognize unknown attacks cooperatively, based on the expendable multi-dimension feature space of attacks.

For example, the procedure of minimize the collaborative attacks such as the blackhole attacks and the wormhole attacks is introduced below. First, the native immune tier detected the selfs, which are normal components of the real mobile ad hoc network. The accurate results for detecting the selfs were used to detect the attacks quickly. Each notebook or ARM had different selfs, and the attack detection of each node was interacted with those of other nodes. When an attack was detected in any node, the information about the attack was sent to the other nodes.

Then the attacks that were detected were recognized by fast search algorithms, and their features were matched or unrecognized in the expendable feature space of all the known attacks. If the search result returned yes, then the attacks were controlled and cleaned in a relatively easy way, and both the features of the attacks were delivered to the relative nodes. If the search result returned no, then the attacks were learnt with some intelligent methods such as enhanced learning from examples and learning based on neural network etc.

4. Analysis of immunization model

Suppose a mobile ad hoc network is denoted as finite immune graph $G=(V, E)$, where V is the vertex or node set, and E is the edge set with $E \neq \phi$. An element in the set V denotes a node in the mobile ad hoc network, and any element in the set E represents the relationship between one node and another. It is assumed that the edges are undirected and the graph is connected. At system initialization, there is no attack, and the mobile ad hoc network is normal with space-time representation of its normal model (Gong et al., 2011). It is also assumed that a unique discrete time order is represented with $t=0, 1, 2\ldots$, though the time properties of some components may be turned back or changed forward with a big step in a local virtual space. Considering the attacks in a sequential order, a node is secure, damaged, or removed at any point in time. When a node is damaged by the attacks, it may be under control of attackers, and thus may attack other nodes as a tool of the attackers. The attacks may remove crucial nodes, and the damaged nodes may be

removed in its immune response in order to be repaired by its backup ones. In Fig. 2, the real mobile ad hoc network has 3 notebook nodes and 2 ARM nodes.

First of all, the set of nodes, which were damaged by the attacks at or before time t, is denoted by D_t. $N(t)$ is used to denote the number of nodes that were damaged at or before time t, and the number of nodes, which were removed or lost by time t, was denoted by $M(t)$. Therefore, $|C_t| = N(t)$, and $N(t)$-$M(t)$ is used to denote the number of nodes that were damaged but have not been removed by time t. For the event that the node was damaged, the degree of node v ($v \in V$) in G is denoted by deg(v), and the set of nodes neighboring with the node v is denoted by $\{v' \mid (v, v') \in E\}$. The time, at which the kth node changes state from secure to damaged (i.e. the kth incident occurs), is denoted by T_k, where $1 \le k \le |V|$. And the identity of the node, which was damaged by the attacks at time T_k, i.e. the kth damaged node, is denoted by node(T_k). Suppose for any sequence of damaged nodes node(T_1), …, node(T_i), …, node($T_{|V|}$), the degree of node(T_i) follows distribution D_i ($1 \le i \le |V|$), which is distributed identically and independently as the degree distribution D of G=(V, E) (Li et al., 2007).

For random variables R_1 & R_2, if Pr[R_1>k] $\ge$ Pr[R_2>k] for any k, then R_1 is called larger (or faster) stochastically than R_2, denoted by $R_1 \succeq_{st} R_2$ (Shaked et al., 1994). Thus, for the sequence of the stochastic intervals between two incidents (e.g. the ith incident and the succeeding incident) occurrences, which are denoted by S_{1i}=T_{i+1} -T_i for i=0, 1,…, $|V|$-1, the sequence S_0, S_1,…,S_k is stochastically decreasing (Li et al., 2007) that is denoted by

$$S_i \succeq_{st} S_{i+1}, i = 0,1,\cdots,|V|-1. \quad (1)$$

This proposition is used to prove that the coordinated attacks become more powerful as more internal nodes are damaged and produce new attacks. Here, the discretization makes T_k follows a discrete Poisson process of success probabilities r_{k-1} for k= 1, … , $|V|$ (Li et al., 2007), and the probabilities r_{k-1} are denoted by

$$r_i = \frac{|V| + d_1 + d_2 + \cdots + d_i - i}{2|E| + |V|}, \quad r_0 = \frac{|V|}{2|E| + |V|}, i = 1,2,\cdots,|V|-1 \quad (2)$$

where $d_j \overset{def}{=} \deg(\text{node}(T_j))$ for j=1, …, $|V|$.

It is assumed that the success probability to detect the damaged node is denoted by p_i and the success probability to cut off the output of the damaged node is denoted by 1- p_i, once the node is found. Therefore, according to (2), the probability r_i with detection is improved by

$$r_i = \frac{|V| + \sum_{j=1}^{i-1} d_j + d_i \cdot (1 - p_i) - i + 1 - p_i}{2|E| + |V|} = \frac{|V| + \sum_{j=1}^{i} d_j - 2p_i - i + 1}{2|E| + |V|}, \quad (3)$$

In general, there are 3 strategies to find the damaged node: (1) attack detection directly by getting and matching the features of the damaged node in the feature space F_B for the incomplete set B of attacks, with measuring errors; (2) unknown attack learning from the feature space F_A for

the complete set A of all known attacks, with uncertain results of detection and recognition; (3) self detection based on the space-time property set F_S of the selfs and the normal model for defining the selfs, and then non-self detection based on the results of the self detection. For strategy 1 and strategy 2, if the node is damaged by known attacks, then the success probability $p_i^{(1)}$ for strategy 1 is denoted by

$$p_i^{(1)} = \frac{|F_B|}{|F_A|} \cdot p_e^{(1)}, i = 1, \cdots, |V|, \tag{4}$$

where the probability of measuring errors for strategy 1 is denoted by $p_e^{(1)}$,and the success probability $p_i^{(2)}$ for strategy 2 is denoted by

$$p_i^{(2)} = p_l \cdot p_e^{(2)}, i = 1, \cdots, |V|, \tag{5}$$

where the probability of measuring errors for strategy 2 is denoted by $p_e^{(2)}$, and the success probability of learning unknown attacks is denoted by p_l. Here, $p_e^{(2)} \approx p_e^{(1)}$, $p_l = 1$.

Thus,

$$p_i^{(1)} \le p_i^{(2)}, \tag{6}$$

$$r_i^{(1)} \ge r_i^{(2)}. \tag{7}$$

Here, for $\gamma \in \{1,2,3\}$, the sequence of geometric success probabilities for detection strategy γ are denoted by $r_1^{(\gamma)}, \cdots, r_k^{(\gamma)}$.

If the node is damaged by unknown attacks, then the success probability $p_i^{(1)}$ for strategy 1 always equals to 0 because the features of the unknown attacks will not be matched in the feature space F_B; to our hope the success probability $p_i^{(2)}$ depends on learning, and mostly $0 = p_i^{(1)} < p_i^{(2)} \le 0.8$ (Meltzoff et al., 2011; Marchiori et al., 2008; Edelman et al., 2007; Behera et al., 2006).

$$0 = \frac{|F_B|}{|F_A|} < p_l \le 0.8. \tag{8}$$

Thus, (6) and (7) are still right.

When the space-time property set F_S is normal with correct data for strategy 3, no matter whether the node is damaged by known attacks or not, the success probability $p_i^{(3)}$ for strategy 3 is denoted by

$$p_i^{(3)} = p_s \cdot p_e^{(3)}, i = 1, \cdots, |V|, \tag{9}$$

where the probability of measuring errors for strategy 3 is denoted by $p_e^{(3)}$, and the normal probability of the selfs is denoted by p_s. Here, $p_e^{(3)} \approx p_e^{(2)} \approx p_e^{(1)}$, $p_s = 1$.

Thus, when the node is damaged by known attacks,

$$p_i^{(3)} \approx p_i^{(2)} \ge p_i^{(1)}, \tag{10}$$

$$r_i^{(3)} \approx r_i^{(2)} \le r_i^{(1)}. \tag{11}$$

But, when the node is damaged by some unknown attacks, according to (8),

$$1 = p_S > 0.8 \geq p_l > \frac{|F_B|}{|F_A|} = 0. \quad (12)$$

$$\therefore\ p_S \cdot p_\varepsilon^{(3)} > p_l \cdot p_\varepsilon^{(2)} > \frac{|F_B|}{|F_A|} \cdot p_\varepsilon^{(1)}. \quad (13)$$

$$\therefore p_i^{(3)} > p_i^{(2)} > p_i^{(1)}, \quad (14)$$

$$\therefore r_i^{(3)} < r_i^{(2)} < r_i^{(1)}. \quad (15)$$

In summary, for any attack,

$$r_i^{(3)} \leq r_i^{(2)} \leq r_i^{(1)}. \quad (16)$$

For $\gamma \in \{1,2,3\}$, the time at which the kth incident due to attacks occurs for detection strategy γ is denoted by $T_k^{(\gamma)}$ (Li et al., 2007), then for k=1, 2, …, |V|,

$$T_k^{(3)} \geq T_k^{(2)} \geq T_k^{(1)}. \quad (17)$$

This proposition is useful, for it inspires us, from the perspective for fighting against the attacks, that detection strategy 3 outperforms detection strategy2, which in turn outperforms detection strategy 1. In fact, because some of the collaborative attacks are known and the others are often unknown, if the space-time property set F_S is normal with correct data, strategy 3 is the best approach to test the attacks; otherwise, strategy 2 is often better than strategy 1, especially in dealing with the unknown attacks.

5. Real experimental results and simulation analysis

The real mobile ad hoc network consisted of 3 notebooks and 2 embedded systems, as shown in Fig. 2. The first embedded system was an ARM9, and the other was an ARM11. The notebooks transferred information each other via the wireless LAN, and their data rates were 54Mbit/s. The ARM9 and the ARM11 transferred information each other via the Zigbee devices, and they connected with the second notebook via the Zigbee devices too. The average data rates of the Zigbee devices were 40Kbit/s, and the maximum data rates were 250Kbit/s.

The blackhole attack was based on the Black Hole exploit kit, which has been used by attackers for major Web-based attacks for last few months. Fig. 2 shows the normal real mobile ad hoc network. The first notebook c_1 was compromised by the blackhole attack, as shown in Fig. 3, and with the Black Hole exploit kit the blackhole attack used the vulnerabilities: CVE-2010-1885, CVE-2010- 1423, CVE-2010-0886, CVE-2010-0842, CVE-2010-0840, CVE-2009-1671, CVE-2009-0927, CVE-2008-2992, CVE-2007-5659 and CVE-2006-0003. The compromised node of notebook misled the other connecting nodes to send information to it without possibility of infection, but no any feedback was returned to the senders.

Fig. 3 – The first notebook compromised by the blackhole attack in the real mobile ad hoc network.

The wormhole attack was implemented with C++ codes, and the second notebook c_2 was compromised by the wormhole attack initially, as shown in Fig. 4 (1). The node c_2 was transferring

the codes of the wormhole attack into the other connecting nodes c_1, c_3, ARM9 and ARM11, keeping old connections.

Fig. 4 (2) shows the final damages of the wormhole attacks on the whole real mobile ad hoc network, i.e. the compromised whole network. In fact, after the compromised notebook transferred the codes of the wormhole attack into the ARM9 and the ARM11 via the Zigbee devices and activated the wormhole attacks on the two embedded systems, the ARM9 and the ARM11 were compromised by the wormhole attacks. Similarly, the compromised notebook by the blackhole attack and the third notebook were compromised by the wormhole attacks, after the code transferring and activation. Though the whole network was compromised by the wormhole attacks in the end, the blackhole attack could quicken the spread of the wormhole attacks by disturbing the routing of information for attack detection.

(1) The first notebook and the second one compromised by the blackhole attack and the wormhole attack respectively.

(2) The final network compromised by the wormhole attacks under the collaborative attacks in the real network.

Fig. 4 –The real mobile ad hoc networks under the collaborative attacks.

When a node was normal, its client program sent normal data such as the data stream from the file data.txt, and the server program of the receiver node got the data of the file data.txt successfully. As one node was compromised by the blackhole attack, the routing table of this node was changed the attack, and so the client program of this node sent no any data to the other nodes. Fig. 5 (1) shows that the immune program detected the blackhole attack by checking the space-time properties of the files with the normal records in the self database. Then the immune program deleted the attacking files and the infected files, and repaired the infected files with the backup system of the normal system. On the other hand, the wormhole attack changed the routing table of the compromised node, and spread the wormhole attack via the client program of this node into other nodes. The server programs of the other nodes received the program file of the wormhole attack from the compromised node, and activated the wormhole attack on those nodes. So those nodes became new compromised nodes of the wormhole attack, and spread this attack into their other nodes until the whole network collapsed. As similar to the blackhole attack, the wormhole attack was detected by the immune program via the normal model, and eliminated finally in Fig. 5 (2). Moreover, the infected files were repaired with the backup system of the normal system, so the whole real mobile ad hoc network recovered the normal state.

(1) Immunization against the blackhole attack in the real mobile ad hoc network.

(2) Immunization against the wormhole attack in the real mobile ad hoc network.

Fig. 5 – Immunization of the real mobile ad hoc network.

Due to the amount limit of notebooks, ARMs and Zigbee devices, the node amount of the real ad hoc network was as small as five, but the node amount of the simulations with the Network Simulator 2.35 (Breslau et al., 2000) was expanded to as large as 20. The simulation parameters were shown in Table 1. The purpose of this experiment was to show that the immune mechanism based on the normal model is deployed in a medium-scale mobile ad hoc network to detect and repair the collaborative attacks such as the blackhole attacks and the wormhole attacks.

Table 1 – Parameter setting of simulations. CBR represents the constant bit rate.

Parameter name	Setting value
Simulation time	10(s)
Number of notebook nodes	10
Number of ARM nodes	10
Initial sum of blackhole node	1
Initial sum of wormhole node	1
Topology	700m*700m
Routing protocol	AODV
Traffic	CBR
Normal packet size	512bytes
Abnormal packet size	1024bytes
Data rates	40K-10Mbit/s
Backup systems	2

In this scenario, 10 notebook nodes and 10 ARM nodes were used, and the notebooks had the same Windows-based backup systems and the ARMs had the same Linux-based backup systems. The basic AODV routing protocol was used and UDP packets were sent and received among the nodes. Based on the AODV routing protocol and the attack features, the protocols of the blackhole attacks and the wormhole attacks were simulated.

The immunization mechanism was used to cut off the connection between the attacked node and other normal nodes and make the attacked node repaired. All simulation runs lasted 10 seconds, and to avoid disturbances from the warm-up period, the first 1 second of the simulation results should be discarded.

Particularly, 1 normal network scenario, 3 different attack scenarios and 2 different anti- attack scenarios were simulated. The effects of single blackhole attack, single wormhole attack and the combined effect of blackhole attack together with wormhole attack on the performance of ad hoc wireless networks were analyzed. Different methods were compared in defending the network against collaborative attacks (Bhargava et al., 2009).

For these evaluations, the reaction time included the detection time and the response time. Different detection approaches spent different time, which might cause important difficulty to eliminate and defend the attacks. In order to improve the accuracy of the test, multiple repeated attacks were conducted to each experiment.

In these experiments, 4 important metrics were evaluated, i.e. packet delivery ratio (PDR), throughput, overhead and end-to-end delay. PDR is denoted with the ratio between the amount of packet delivered at the destination node and the whole amount of sent packets by the source node. Throughput and end-to-end delay are used to show the network performance degradation. Besides,

overhead is represented with the fraction of all control packets sent during the simulation time out of the total amount of packets transmitted. Fig. 6 shows the packet delivery ratio (PDR) in four types of networks. The first network was normal one; the second was damaged by the blackhole attack on a node; the third was damaged by the wormhole attack on another node and the last one was damaged by the collaborative attacks.

Fig. 6 - Packet delivery ratios of the networks under attacks including collaborative attacks.

The networks under the blackhole attack or the collaborative attacks had lower packet delivery ratios than the normal network, because the blackhole attack destroyed the local network communication. In fact, the wormhole attack enhanced the packet delivery ratio and transferred the wormhole programs to other normal nodes in the nine seconds in Fig. 6. So the packet delivery ratio of the network under the wormhole attack was even higher than that of the normal network until the abnormal wormhole transferring caused the network collapse alike in Fig. 5 (2) after the nine seconds. The four curves in different positions show that the collaborative attacks combined the hidden harms of the single wormhole attack and the communication destroying of the single blackhole attack.

Comparing with the packet delivery ratios of the network under the collaborative attacks and the network based on the regular IDS against the attacks, the packet delivery ratio of the network with cooperative immunization was higher, as shown in Fig. 7. The possible reason for this result is that the cooperative immunization was faster and more effective against the collaborative attacks than the regular IDS.

Fig. 7 - Packet delivery ratios of the networks defending against collaborative attacks.

For comparing the performances of the regular IDS and the cooperative immunization, the throughputs of the connections in the two networks were analyzed in Fig. 8. By this outcome from 2 second to 4 second, it is sure to affirm that the regular IDS caused higher throughput than the cooperative immunization due to the harmful expansion of wormhole nodes. The node under wormhole attacks was isolated and the normal nodes were protected by the immune network based on the normal model. After 4 second in Fig. 8, the two throughputs of the connections in the different networks were almost same, and the immune network's throughput is slightly higher than the IDS-based network's throughput.

Fig. 8 - End-to-end throughput.

The next metric evaluated was the network overhead, which shows how much of control packets were generated within the network, as shown in Fig. 9. The immunization against the collaborative attacks always performed best, and the normal network performed better in average than both the network under the collaborative attacks and the regular IDS against the collaborative attacks.

The last observed metric, the end-to-end delay, is shown and compared in Fig. 10.

Fig. 9 - Overall overhead.

Fig. 10 - End-to-end delay.

The results in Fig. 10 were calculated by taking the average of the end-to-end delay of the incoming packets at the receiver. As same as the previous, the end-to-end delay stresses the better performance for the mobile ad hoc network by the immunization rather than the regular IDS against the collaborative attacks.

Overall, the NS2-based simulations results allow affirming that it is important and useful for the mobile ad hoc network to utilize the cooperative immunization for security. Based on analyzing the experiment results, the immunization has three advantages than the regular IDS. First, the immunization is able to isolate the nodes under attacks by the network reconfiguration; second, the immunization can identify the nodes under attacks by detecting the non-selfs and the selfs based on the normal model, which is very useful and crucial for controlling and eliminating the fast expansion of the active attacks such as the wormhole attacks; finally, the immunization is of new powerful learning mechanism for defending the networks, called as immune learning.

6. Conclusions and future works

Some important properties and mechanisms of cooperative immunization were proposed to defend the ad hoc network under collaborative attacks. New tri-tier cooperative immunization based framework was designed to detect and recognize the collaborative attacks in mobile ad hoc networks such as the real mobile ad hoc network of ARMs and notebooks. The performance of the proposed framework was analyzed in term of the packet delivery ratios, the throughput, and the traffic overhead of the system. The real experiments and simulation results confirm effectiveness of the proposed cooperative immunization model in detecting and mitigating the collaborative attacks from disrupting the protected mobile ad hoc networks such as the real mobile ad hoc network of ARMs and notebooks.

For future works, it is interesting to improve the protocols of immunization by increasing the accuracy and speed of the adaptive immunization in dealing with unknown attacks. Evaluations of the issues such as efficiency, space-time identification, complexity, optimization, and consumption are also left for future work.

Acknowledgements

The work was supported in part by grants from Natural Science Foundation of Shanghai (08ZR1400400), the Shanghai Educational Development Foundation (2007CG42), the National Natural Science Foundation of China (60874113), NSF-0242840, & NSF-0219110. This material is partly based on research sponsored by Air Force Research Laboratory under agreement number FA8750-10-2-0152 & the U.S. Department of Homeland Security under Grant Award Number 2006-CS-001- 000001, under the auspices of the Institute for Information Infrastructure Protection (I3P) research program. The I3P is managed by Dartmouth College. The U.S. Government is

authorized to reproduce and distribute reprints for Government purpose notwithstanding a copyright notation thereon. The views and conclusions contained in this document are those of the authors and should not be interpreted as necessarily representing the official policies, either expressed or implied, of the U.S. Department of Homeland Security, the I3P, or Dartmouth College.

References

Balthrop J, Forrest S, Newman MEJ, et al. Technological Networks and the Spread of Computer Viruses. Science, 2004, 304 (5670): 527-529.

Behera L, Kumar S, Patnaik A. On Adaptive Learning Rate That Guarantees Conver- gence in Feedforward Networks. IEEE Transactions on Neural Networks, 2006, 17(5): 1116 - 1125.

Bhargava B, Oliveira R, Zhang Y, et al. Addressing Collaborative Attacks and Defense in Ad Hoc Wireless Networks. In: 29th IEEE International Workshops on Distributed Computing Systems, 2009, 447-450.

Bhargava B, Zhang Y, Idika N, Lilien L, et al. Collaborative attacks in WiMAX networks. Security and Communication Networks, 2009, 2(5): 373–391.

Bordon Y. Mucosal immunology: Acid attack. Nature Reviews Immunology, 2011, Vol. 11, 156.

Breslau L, Estrin D, Fall K, et al. Advances in Network Simulation. IEEE Computer, 2000, 33 (5): 59-67.

Cuppens F, Miege A. Alert correlation in a cooperative intrusion detection framework. In Proc. of IEEE Symposium on Security and Privacy, Toulouse, 2002.

Dasgupta D, González F. An immunity-based technique to characterize intrusions in computer networks. IEEE Transactions on Evolutionary Computation, 2002, 6(3): 281-291.

Douceur J. The Sybil attack. In the First International Workshop on Peer-to-Peer Systems, 2002

Edelman G. Learning in and from Brain- Based Devices. Science, 2007, 318: 1103- 1105.

Esponda F, Forrest S, Helman P. A Formalframework for positive and negative detection. IEEE Transactions on Systems, Man and Cybernetics. 2004, 34(1): 357-373.

Garcia-Osorio A, Loo-Yau JR, Reynoso- Hernandez JA. A GaN class-F PA with 600 MHz bandwidth and 62.5% of PAE suitable for WiMAX frequencies. 2010 IEEE International Microwave Workshop Series on RF Front-ends for Software Defined and Cognitive Radio Solutions (IMWS), 2010,1-4.

Gong T, Cai ZX. Anti-Worm Immuni- zation of Web System Based on Normal model and BP Neural Network. Lecture Notes in Computer Science, 2006, Vol. 3973, 267-272.

Gong T, Cai ZX. Tri-tier Immune System in Anti-virus & Software Fault Diagnosis of Mobile Immune Robot Based on Normal Model. Journal of Intelligent and Robotic Systems, 2008, 51(2): 187–201.

Gong T, Li L, Du CX. Modeling and Simulation of Visual Tri-Tier Immune System. Applied Mechanics and Materials, 2011, Vols. 48-49, 701-704.

Gros1 P. In self-defense. Nature Structural and Molecular Biology, 2011, online

Hussain A, Heidemann J, Papadopoulos C. COSSACK: coordinated suppression of simultaneous attacks. In DISCEX, 2003.

Kephart J. Learning from Nature. Science, 2011, 331: 682-683.

Li X, Xu S. A stochastic modeling of coordinated internal and external attacks. Technical Report. 2007, Available at: http:// www.cs.utsa.edu/˜shxu/collabora- tive-attack-model.pdf

Lin W, Xiang L, Pao D, Liu B. Collaborative Distributed Intrusion Detection System. 2nd International Conference on Future Generation Communication & Networking, 2008, Vol. 1, 172-177.

Marchiori D, Warglien M. Predicting Human Interactive Learning by Regret- Driven Neural Networks. Science, 2008, 319: 1111-1113.

McCune JM, Shi E, Perrig A, Reiter MK. Detection of denialof-message attacks on sensor network broadcasts. In IEEE Symposium on Security & Privacy, 2005.

Meltzoff A, Kuhl P, Movellan J, et al. Foundations for a New Science of Learning. Science, 2009, 325: 284-288.

Moore D, Paxson V, Savage S, et al. Inside the slammer worm. IEEE Security & Privacy, 2003, 1(4): 33–39.

Motorola Inc. WiMAX security for real- world network service provider deploy- ments. White Paper, 2007.

Ourston D, Matzner S, Stump W, et al. Coordinated internet attacks: responding to attack complexity. Journal of Computer Security, 2004, 12(2): 165–190.

Ramaswamy S, Fu H, Nygard K. Effect of cooperative blackhole attack on mobile ad hoc networks. In ICWN, 2005.

Schuba CL, Krsul IV, Kuhn MG, et al. Analysis of a denial of service attack on TCP. In IEEE Symposium on Security & Privacy, 1997.

Shaked M, Shanthikumar J. Stochastic Orders and Their Applications. Academic Press, San Diego (CA), 1994.

Sukwong O, Kim HS, Hoe JC. Commercial antivirus software effectiveness: an empirical study. IEEE Computer, 2011, 44(3): 63-70.

Wang W, Bhargava B, Lu Y, Wu X. Defending against wormhole attacks in mobile ad hoc networks. Wireless Communications & Mobile Computing, 2006, 6(4): 483–503.

Yang J, Ning P, Wang XS, et al. CARDS: A distributed system for detecting coordinated attacks. In Proc. of IFIP TC11 16th Annual Working Conference on Information Security, 2000.

Yu H, Kaminsky M, Gibbons PB, et al. SybilGuard: defending against Sybil attacks via social networks. In ACM SIGCOMM, 2006.

Yu-Sung W, Foo B, Mei Y, Bagchi S. Collaborative intrusion detection system (CIDS): a framework for accurate and efficient IDS. In Proc. Computer Security Applications Conference (ACSAC '03), 2003.

Zhou JS, Chen Z, Jiang W. Probability based IDS towards secure WMN. 2010 2nd International Workshop on Intelligent Systems and Applications, 2010, 1-4.

Ziv1 Y, Ron1 N, Butovsky1 O, et al. Immune cells contribute to the maintenance of neurogenesis and spatial learning abilities in adulthood. Nature Neuroscience, 2006, Vol. 9, 268-275.

Tao Gong is an associate professor in AI and security at Donghua University, China (http:// autodept.dhu.edu.cn/taogong), and a visiting scholar at Purdue University, USA, Dept. of Computer Science, and CERIAS. He is a Life Member of Sigma Xi, The Scientific Research Society, the General Editors-in-Chief of the first leading journal *Immune Computation* in its field, and editorial board member of some international journals. He received a Ph. D. degree and a M.Sc. degree from Central South University in 2007 and 2003 respectively. His research interests are related to applications of immune computation in the area of network security.

Bharat Bhargava is a professor at Purdue University, USA, Department of Computer Science, and CERIAS. He is an IEEE Fellow and IETE Fellow, and serves on seven editorial boards of international journals. He received a Ph. D. degree from Purdue University in 1974. His research interests are related to security and privacy issues in distributed systems.

Jiajia Zhou is a master student at Donghua University, China. Her research interests are related to security in networks of embedded systems and network intelligence.

Mehdi Azarmi is a doctoral student at Purdue University, USA, Department of Computer Science. His research interests are related to advanced techniques in the area of network security, especially attack detection.

Changxing Du is a master student at Donghua University, China. His research interests are related to advanced techniques in the area of embedded systems, especially security in the core of the embedded systems.

Figure
Click here to download high resolution image

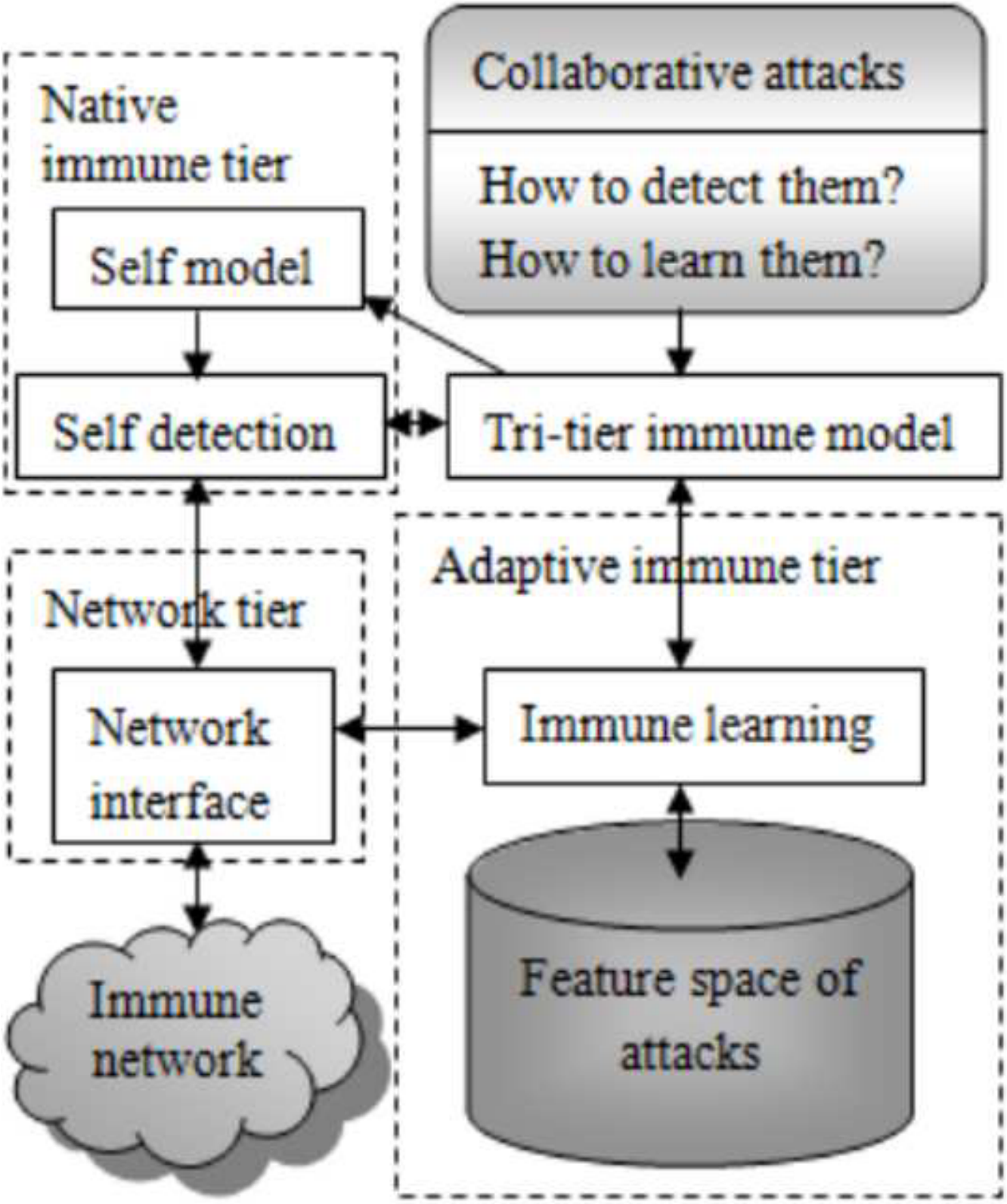


Figure
Click here to download high resolution image

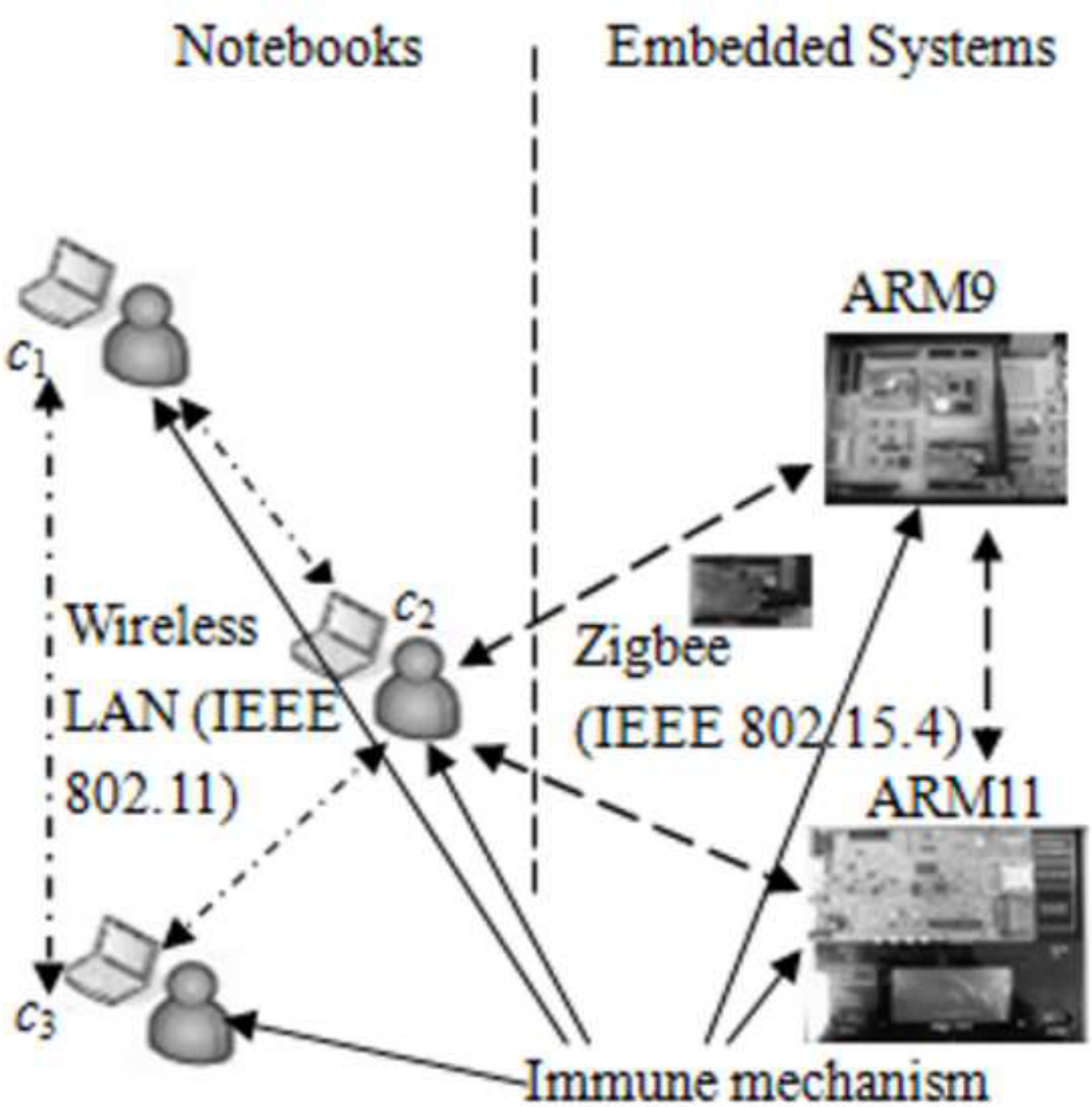


Figure
Click here to download high resolution image

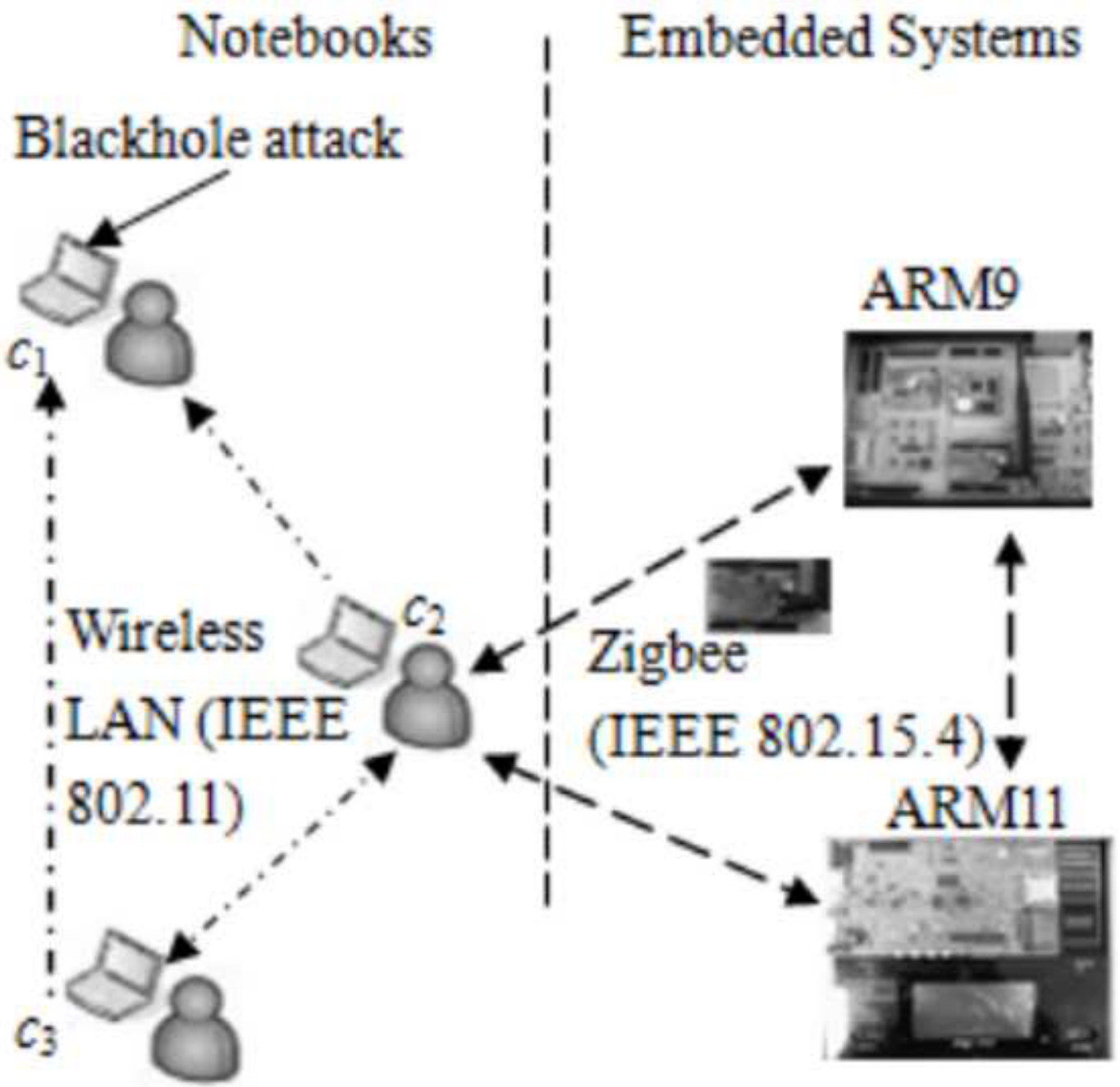


Figure
Click here to download high resolution image

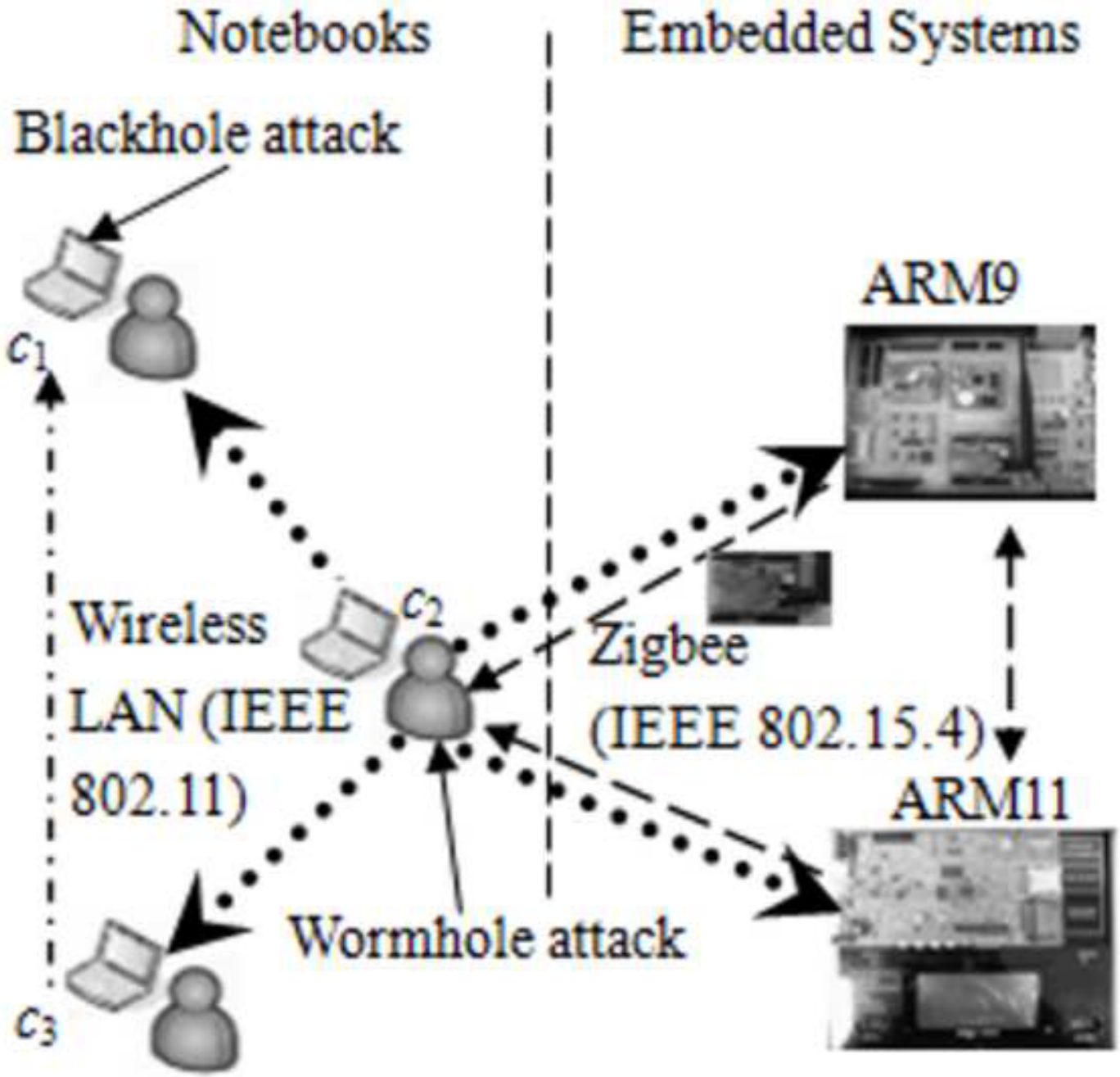
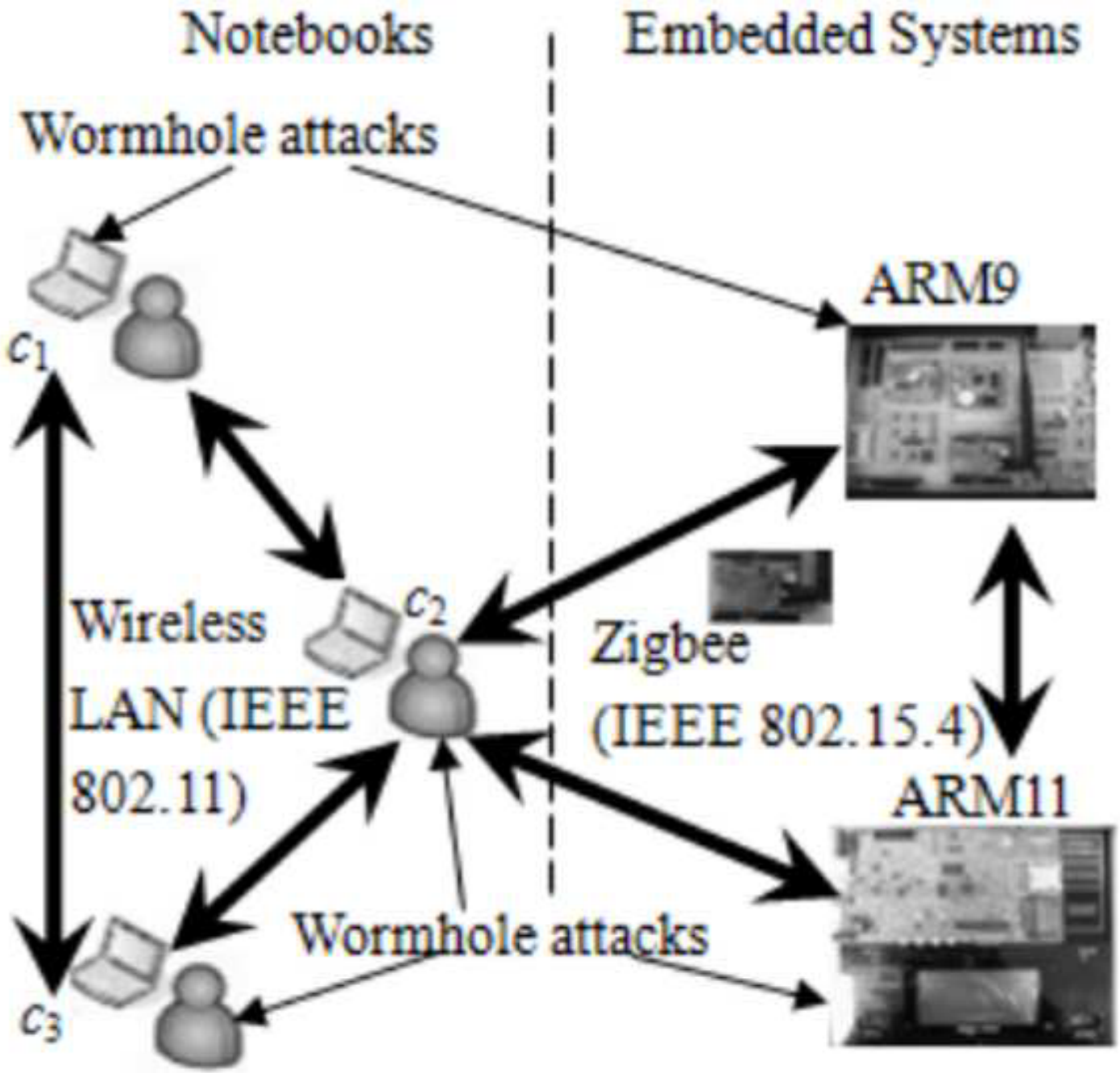
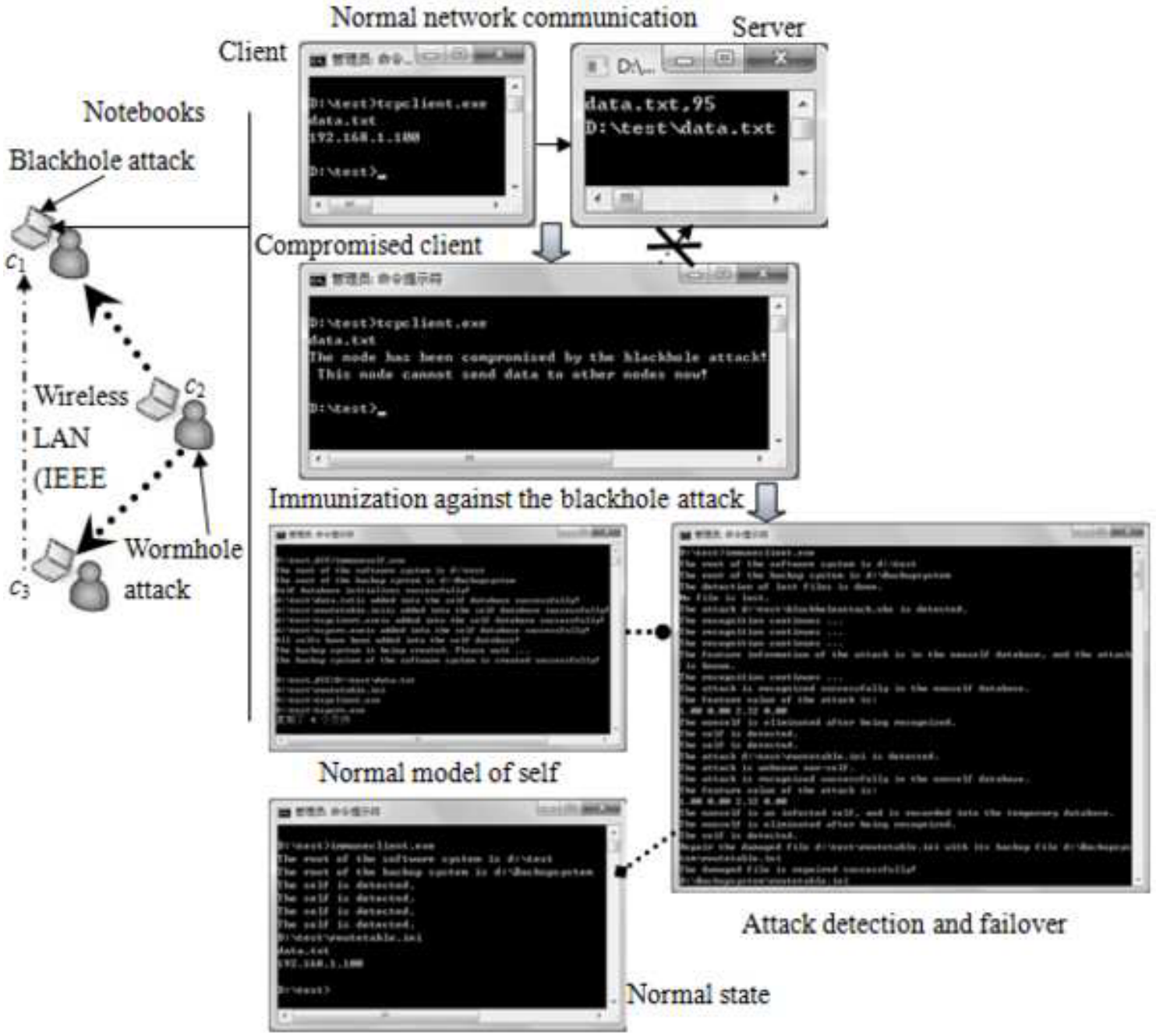


Figure
Click here to download high resolution image



Figure

Click here to download high resolution image



Figure

Click here to download high resolution image

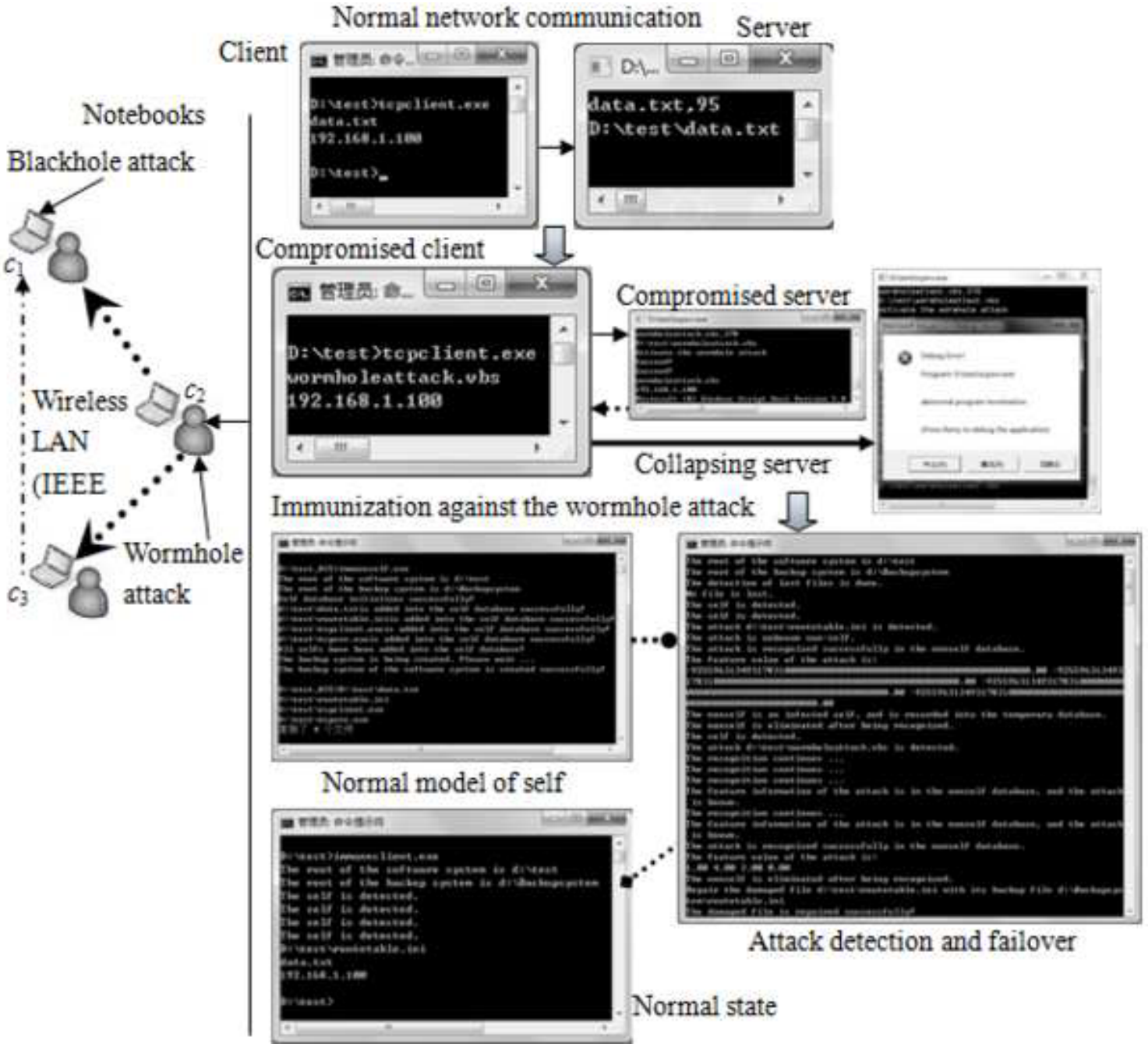


Figure
Click here to download high resolution image

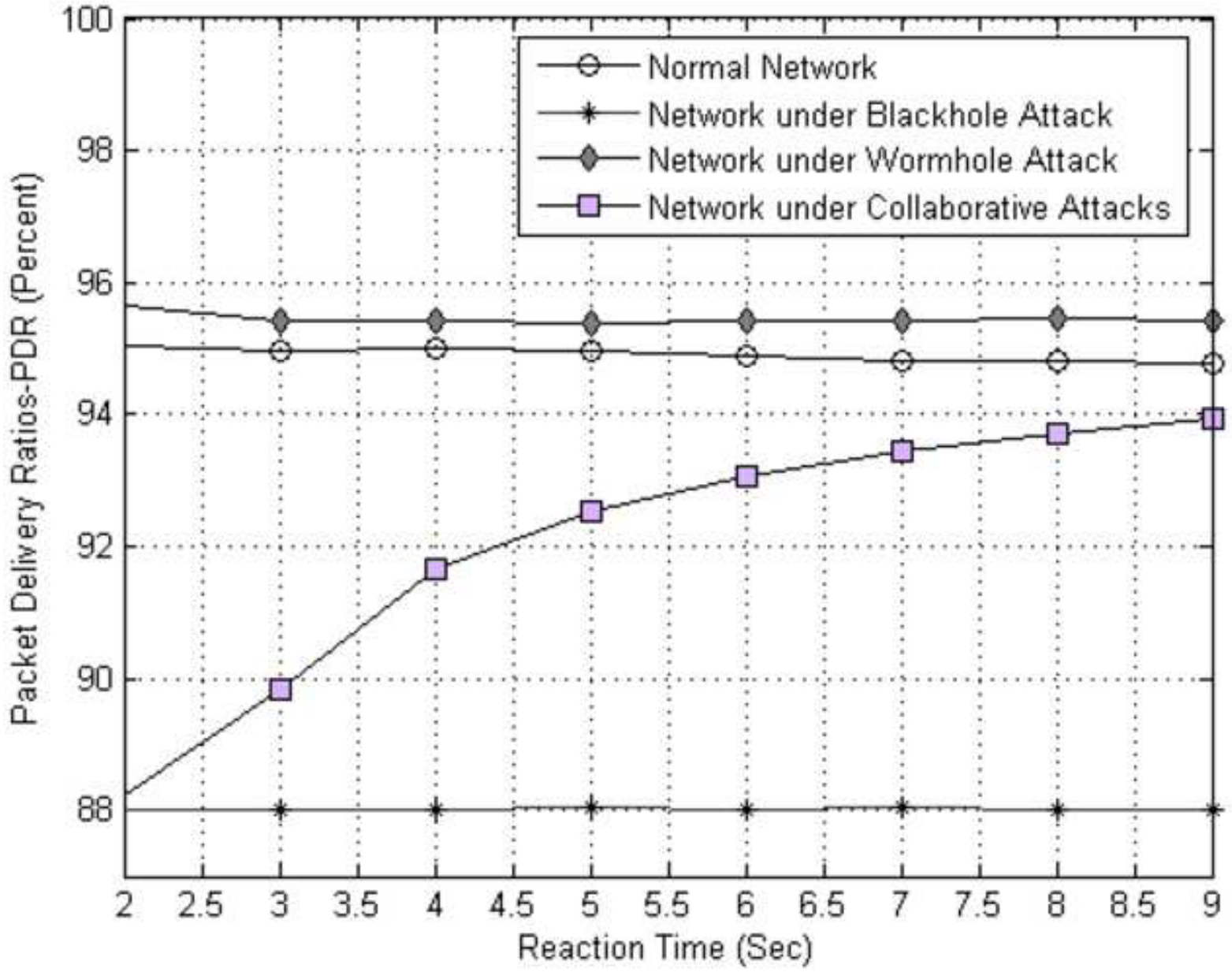
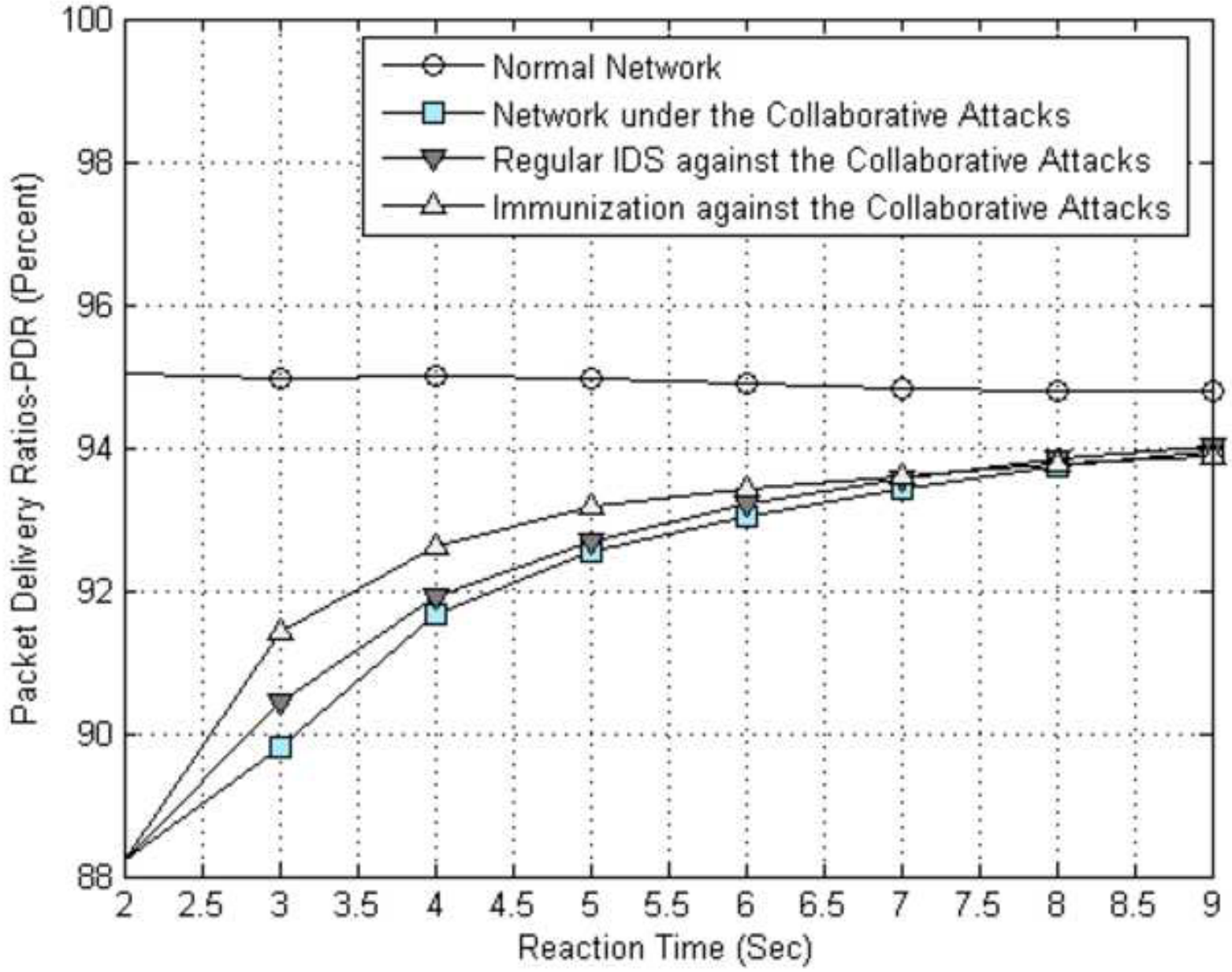


Figure
Click here to download high resolution image



Figure

Click here to download high resolution image

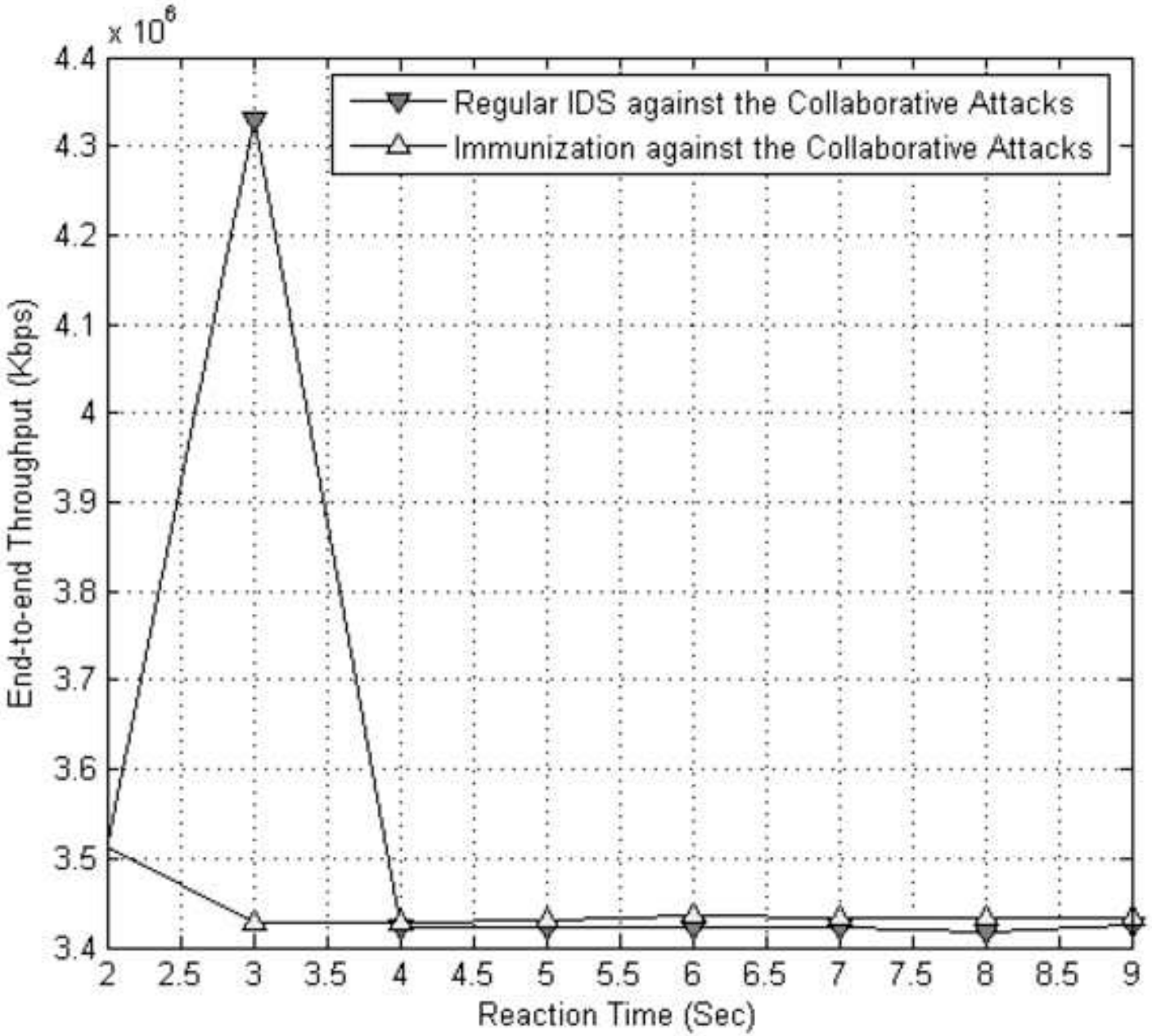


Figure
Click here to download high resolution image

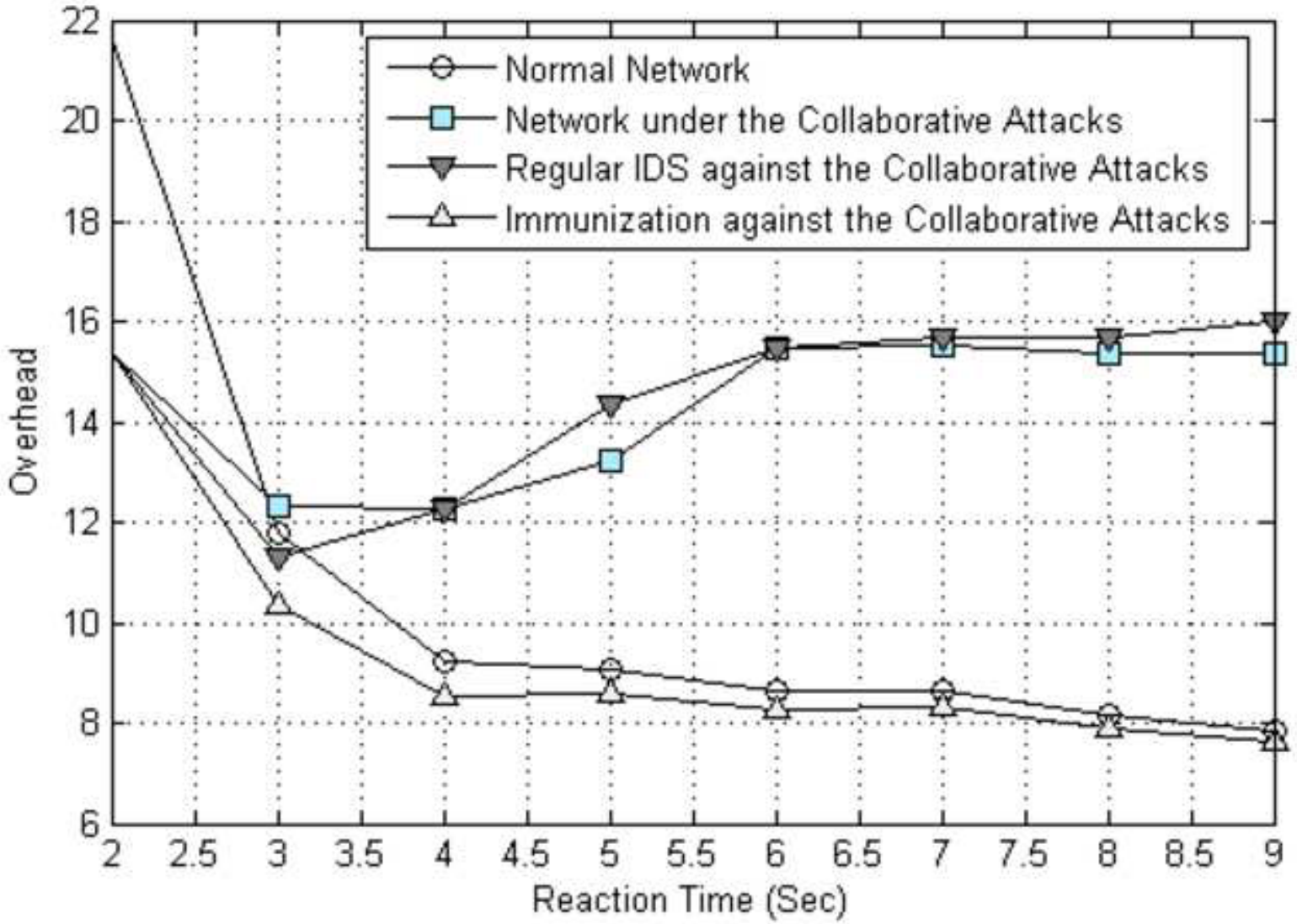


Figure
Click here to download high resolution image