A Traffic Based Lightweight Attack Detection Scheme for VoLTE

Na Ruan, Qi Hu, Lei Gao, Haojin Zhu, Qingshui Xue, Weijia Jia and Jingyu Cui
Shanghai Jiao Tong University, China

***Abstract*—With rapid growth of LTE network and Voice-over-LTE(VoLTE), detecting and preventing security threats like Denial of Service attack becomes a necessary and urgent requirement. VoLTE is an voice solution based on Internet Protocol and 4G LTE technology, at the same time exposing many vulnerabilities when using packet-switched network. There are many heavy weighted detection systems using content analysis, while high demands of computing resource constraint their practical use. In this paper, we propose a lightweight detection scheme for VoLTE network security, based on analysis of data traffic flow. To optimize parameters in our scheme, we formulate a Bayesian game model. Bayesian game has the features of incomplete information and asymmetry, similar to practical attack-defense model. Besides, The dynamic Bayesian game is more realistic, since both sides can update believes about their opponents. Simulation results provide some guidances on parameter selection, as well as verifying the superiority of our scheme.**

I. Introduction

As the dedicated voice solution for LTE, VoLTE is an implementation of Voice-over-IP, which uses packet-switched networks for data transmission. Based on Internet technology, VoLTE provides obvious benefits over its former generations 2G/3G call service, in respects of higher Quality of Service (QoS), larger call capacity, shorter start-up time and better interoperability [1].

However, as VoLTE shifts circuit-switched scheme to packet-switched, which provides a higher openness to operating system, there are new security threats to both consumers and operators. So far there's no effective verification for authenticity of VoLTE signal and data. Major attacks, such as Denial of Service (DoS) attack, free data attack and over-charging attack, are caused by injecting purposive or useless packets into control plane or data plane [2]. Besides, signaling bearer in control plane of VoLTE has the highest priority level whereas data bearer (e.g. web searching, video streaming) has the lowest one; and voice bearer has guaranteed bit rate, whereas data bearer belongs to the non-guaranteed bit rate category. All these privileges aims at providing VoLTE with higher QoS. However the high QoS may restrain normal data access [3], making these attacks more destructive and easier to implement.

Actually, the security vulnerabilities of VoLTE essentially lie in the lack of verification of transmitted data. So a thorough solution to these threats is an authentication subsystem for transmission details, such as source address, destination address, protocol type. Nevertheless, content based verification requires real-time monitoring and analysis, which brings challenges of high demand for computing resources [4]. Even if it's performable, the high cost will still prevent it from practical use, especially for some lightweight distributed systems. Meanwhile, the common feature of these attacks is a large amount of data traffic, which provides another clue to lightweight detection.

Besides, there's no effective approach to optimize and evaluate detection schemes so far. Recently, game theory has been successful in analysis of network security, especially in attack defense models. A defense system usually involves multiple types of participant, which cooperate with or oppose to each other. Game theory helps study the action and relationship of cooperators or opponents. In particular, Bayesian game formulates a partially rational model where players only have bounded knowledge. This incomplete information feature accurately describes the reality in VoLTE networks.

To address these challenges, we propose a lightweight Traffic Based Detection System (TBDS). Our contributions can be summarized as follow:

1) To balance the requirement of detection accuracy and cost sensitiveness in VoLTE, we propose a TBDS to detect attacks by monitoring peak value and variation trend of data volume.
2) To evaluate the TBDS, we formulate a Bayesian game model for a practical VoLTE network. We theoretically analyse the equilibrium in static game model, and implement the simulation on dynamic game model.
3) Based on various simulation results, we verify the advantages of our detection system, and give advices on threshold settings.

The remainder of the paper is organized as follows. In section II, we introduce some previous works in this field and discuss how our work differs from other related works. In section III, we show the detail of our proposed Traffic Based Detection System to help detect attacks in VoLTE network. We present the game theoretical approach in section IV. The evaluations of our scheme are shown in section V. The last section draws a conclusion of our work.

II. Related Work

A. Vulnerabilities in VoLTE

In traditional circuit-switched voice solution, both signal and data are generated and managed within chipset, which

978-1-5090-1328-9/16/$31.00 ©2016 IEEE

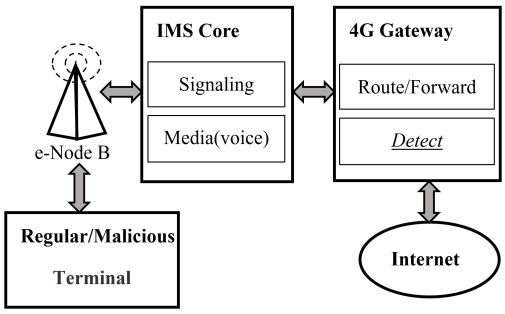


Fig. 1: Structure of practical VoLTE network.

protects transmission from being interfered. However, Li C Y *et al*. [1] found the openness of VoLTE control-plane to software (e.g. operating system and apps) makes it defective to attacks. As long as attackers get the access authority, they can inject data packets into signaling bearers to implement DoS, shutting down ongoing data service at the victim. And high QoS of VoLTE makes DoS attacks more harmful.

Guan-Hua Tu *et al*. [5] pointed out a threat that VoLTE signaling may be manipulated maliciously. For instant, the handshake process in Session Initiation Protocol (SIP) won't finish until the caller send *SIP UPDATE*, a confirming message [6]. A malicious caller may send *CANCELING* instead to launch a silent call attack. Such successive attack will speed up consumption of power or even cause call blocking, while the victim has no idea about it.

Accordingly, researchers proposed some countermeasures, such as stricter routing regulation, verification and authorization, improving transmission protocols, chipset access enhancement. However, many of these remedies are generally put forward with no implementation detail, or even not feasible due to the limitation of market and policies.

B. Game Theroy in Network Security

It is widely investigated that a large number of game models have been applied to evaluate security issues in network (e.g. repeated game, evolutionary game, stackelberg game) [7]. All these games can be categorize into static/dynamic, complete/incomplete information, cooperative/non-cooperative, symmetric/asymmetric, zero-sum/non-zero-sum, simultaneous/sequential, finitely/infinitely, etc. [8]

Liu Y *et al*. [9] proposed a Bayesian game approach for Intrusion Detection System in Ad Hoc Networks. The Bayesian game model is used for a dynamic process here, where the defender continually updates belief about the opponent.

III. Traffic Based Attack Detection Model

In this section, we propose a lightweight Traffic Based Detection System (TBDS) as a subsystem in VoLTE network. The peak value and trend feature of data traffic are used to analyse the probability of attack , then optimize the parameters in detection system. The TBDS and model of VoLTE network are illustrated in Session III.*A* and III.*B*.

TABLE I: Notations in TBDS

t_0	length of one detection period
M	number of sampling point in one detection period
V	peak traffic value of a practical bearer
V_n	peak traffic value of a normal bearer
V_a	peak traffic value of a attacking bearer
V_0	threshold of peak value
$\boldsymbol{F}$	feature of traffic curve of a practical bearer
$\boldsymbol{F}_n$	feature of traffic curve of a normal bearer
$\boldsymbol{F}_a$	feature of traffic curve of a attacking bearer
$\boldsymbol{F}_0$	threshold of curve feature

A. Traffic Based Detection System

The TBDS exploits an lightweight traffic based scheme, which analyses the peak value and trend feature of traffic to distinguish attacks. The information of traffic is much less than that of content, which assures the lightweight feature of TBDS.

Notations in the TBDS are explained in TABLE I. In order to realize the detection process, we simulate practical curves of traffic volume for a period of time. These curves are based on the attacker's action. The attacker will launch an attack with a probability p. If there's an attack from the attacker, traffic volume of corresponding connection V will exceed normal value V_n. Each curve is separated into sequential stages and the TBDS detects attacks based on data volume in each stage.

In our simulation, we assume that the traffic volume of a normal bearer is stable and restrained to a limited range. Besides, we also assume that the traffic volume will increase linearly when there's an attack. Thus the TBDS applies linear fitting to get the slope k of the volume curve. The slope denotes the increment speed of traffic volume, and the slope of an attack bearer will obviously larger than that of a normal one. Researches [1] [12] have shown that in normal scenario, the data volume of a VoLTE bearer are very limited, typical *20-60 kbps*, while an attack would make a sudden drastic fluctuation. As long as the detection interval is short enough, we can always regard the growth as linear. Thus attack detection via analysis of peak value and trend feature is feasible. There are two criterions for attack detection:

1) Peak value V exceeds a given threshold V_0;
2) Feature $\boldsymbol{F}$ exceed a given threshold $\boldsymbol{F}_0$. $\boldsymbol{F}$ is a feature vector generated by fitting of the traffic volume curve.

Only if both two criterions are satisfied, will the bearer be judged as attacking. The threshold V_0 is decided by peak value V_n and V_a, and the threshold $\boldsymbol{F}_0$ is decided by features $\boldsymbol{F}_n$ and $\boldsymbol{F}_a$. Specifically, we designate slope k as feature $\boldsymbol{F}$. After detection process, the TBDS will take corresponding measurements to maximize its payoff(*i.e.* shut down attacking bearers).

The detection system works as Algorithm 1:

Algorithm 1 Detection Procedure

Input:

$V(t)$, continuous traffic volume of the bearer, $0 < t < t_0$;
V_0, threshold of traffic peak value;
k_0, threshold of traffic curve slope;
M, number of sampling point;

Output:

T, estimated bearer type(*T(attacking)* = 1, *T(normal)* = 0);

Get sampling value of traffic volume:
$\boldsymbol{V} = V(t)\sum_{i=1}^{M}\delta(t-\frac{t_0}{M}), V_i$ is a component of $\boldsymbol{V}$, $1 \leq i \leq M$.
T = 0, N = length($\boldsymbol{V}$);
V_{peak} = Max(V_i)
if $V_{peak} > V_0$ **then**
    $V_{avg} = \frac{1}{N}\sum_{i=1}^{M} V_i$
    $k = \frac{\sum_{i=1}^{M}(V_i - V_{avg})(i-\frac{M}{2})}{\sum_{i=1}^{M}(i-\frac{M}{2})}$
  if $k > k_0$ **then**
    T = 1;
  end if
end if
return T

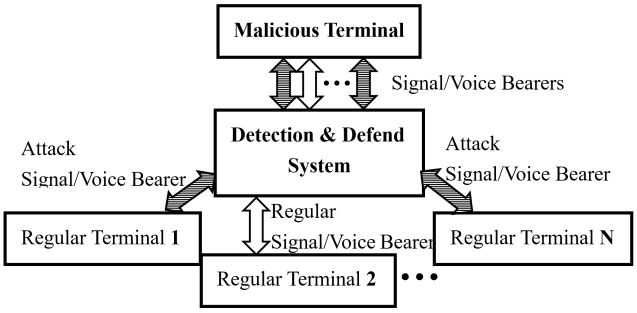


Fig. 2: Structure of the attack defense system.

B. TBDS in VoLTE Network

We merge the TBDS into a VoLTE network model to optimize the parameters in it. In consideration of the VoLTE network structure, we suggest the operators to add the TBDS to 4G gateway, since operators have better control on technology and operation procedure. Besides, 4G gateway is a critical node for routing and forwarding in whole network [10], and more capable of counting data traffic. It's also feasible to applied this TBDS to IP Multimedia Subsystem (IMS) core in VoLTE network, since IMS is a standard architecture for delivering IP multimedia services [11]. All signaling and media traffic in VoLTE must be processed by IMS core. The structure of whole transmission system with detection subsystem in 4G gateway is shown in Fig.1.

Consider a VoLTE network including *N+2* nodes. There are *N* regular nodes which represent normal terminal equipments, a defending node for TBDS and an attacking node for the potential malicious terminal. The relationship among these nodes are illustrated in Fig.2.

The potential malicious terminal can launch attacks toward any normal terminal through a VoLTE bearer. The bearers are dedicated connections for VoLTE, represented by bidirectional arrows in Fig.2. There are two types of bearer: attacking bearer (striped arrow) and normal bearer (blank arrow).

The TBDS plays a connective role in VoLTE network, since each bearer from the potential malicious terminal must go under the monitoring of the TBDS.

The TBDS can also be used as lightweight module in a hybird detection system. Compared to content based heavyweight detection schemes, which verify details in VoLTE packets such as address, port number and transmission protocol [4], TBDS achieves a lower hardware requirement with the side-effect of a lower accuracy. Considering the rapid growth of VoLTE traffic and operators' preference for a lower cost, TBDS has a advantage over those content based algorithms.

IV. Bayesian Game Model

We propose to use Bayesian game model in evaluation of VoLTE attack-defense system. Both static and dynamic Bayesian game are used here: static model to analyse the equilibrium and dynamic model to simulate the game evolving process. The advantages of Bayesian game for this attack-defense model are:

1) *Non-cooperation*: Bayesian game model can be applied to a pair of opponents;
2) *Incomplete information*: Bayesian game simulates the scenario where each side has partial information about the opposite;
3) *Dynamics*: dynamic Bayesian game reflects the dynamic update process;
4) *Asymmetry*: different characteristics of attacker and defender can be represented by parameter setting.

All these features are in accord with the a practical attack-defense system.

A. Static Bayesian Game Model

In static Bayesian game, we establish a incomplete information game model [8], where node B (defending node) assumes that node A (attacking node) has a prior probability μ to be malicious, and node A assumes that node B has a prior probability ν to be defensive. This assumption bases on the fact that both nodes don't know the exact type of the opposite side. There's a nature node W to represent the initial state of node A and B. In order to analyse the payoffs, we use some notations to represent parameters in game model as illustrated in TABLE II.

When the strategy is (*Attack*, *Defend*), the probability of a successful attack is $(1 - P_d)$, and probability of an attack failure is P_d. Thus the gain of node A is $(1-P_d)B_a - P_d L_a$, and we remove the cost C_a to get the overall payoff. Node B's gain is $P_d B_d + (P_d - 1)L_d$, and we remove the cost C_d to get node B's payoff.

When the strategy is (*Not attack*, *Defend*), node A's payoff is 0. Node B has a probability of P_f to make a false alarm, which costs node B an additional loss, -$P_f B_d$.

TABLE II: Notations in Bayesian Game

μ	expected value of node A being malicious
ν	expected value of node B being defensive
p	conditional attack probability of a malicious node
q	conditional defense probability of a defensive node
P_d	true positive rate of TBDS
P_f	false positive rate of TBDS
B_a	gain of a successful defense
B_d	gain of a successful attack
L_a	loss of a failed attack (being successfully defended)
L_d	loss of being attacked without successful defense
C_a	cost of an attack
C_d	cost of a defense

TABLE III: Payoffs Matrix

Payoff of Attacker\Defender	Defend	Not defend
Attack	$(1-P_d)B_a - P_dL_a - C_a$, $P_dB_d + (P_d-1)L_d - C_d$	$B_a - C_a$, $-L_d$
Not Attack	0, $-P_fB_d - C_d$	0, 0

When the strategy is (*Attack*, *Not defend*), node A will successfully launch the attack to get a gain of B_a, and node B will get a loss of L_d.

When the strategy is (*Not attack*, *Not defend*), both sides will have no gain or cost. Thus the payoff on both sides is 0. The payoffs in above four situations are summarized in TABLE III.

Given the payoffs, we can analyse the Bayesian Nash Equilibrium (BNE), provided μ and ν are common prior information. The analysis is based on categories of node A's strategies:

1) *Node A launches an attack as long as it's malicious.* In this case, node B's expected payoffs of *Defend* E_D and *Not defend* E_{ND} are

$$E_D = \mu(P_dB_{ds} + (P_d-1)L_d - C_d) + (1-\mu)(-P_fB_{ds} - C_d),$$

$$E_{ND} = \mu(-L_d) + (1-\mu)(0) = -\mu L_d.$$

Let

$$E_D = E_{ND},$$

, and we get the focal point of node B is

$$\mu_0 = \frac{P_fB_d + C_d}{P_d(B_d+L_d) + P_fB_d}.$$

Thus, node B's strategy is (*Defend* if defensive and $\mu > \mu_0$, *Not defend* if regular or $\mu < \mu_0$). But if $\mu > \mu_0$, node A's dominant strategy is *Not attack* because any attack will probably be detected. In a word, ((*Attack* if malicious, *Not attack* if regular), *Not defend*) is a BNE when $\mu < \mu_0$.

2) *Node A don't attack even if it's malicious.* In this case, the node B's dominant strategy is always *Not defend*. Then Node A's dominant strategy switches to *Attack* if it's malicious. Thus, this is not a BNE.
3) *Node A launches an attack with a probability p if it's malicious.* When $\mu > \mu_0$, there's no pure strategy BNE as we discussed above. We can set conditional attack rate p and conditional defend rate q as illustrated in TABLE II to get a mixed BNE. Then node A's payoff is

$$E_A = \mu\nu q((1-P_d)B_a - P_dL_a - C_a) + \mu(1-\nu q)(B_a - C_a),$$
$$E_{NA} = 0.$$

And node B's payoff is:

$$E_D = \mu p(P_dB_d + (P_d-1)L_d - C_d) + \mu(1-p)(-P_fB_d - C_d) + (1-\mu)(-P_fB_d - C_d), \quad (1)$$
$$E_{ND} = -\mu pL_d. \quad (2)$$

The stable state requires that there's no difference between payoffs of *Attack* and *Not attack*, *Defend* and *Not defend*:

$$E_A = E_{NA},$$
$$E_D = E_{ND},$$

then we get

$$p_0 = \frac{P_fB_d + C_d}{(P_d(B_d+L_d) + P_fB_d)\mu}, \quad (3)$$
$$q_0 = \frac{B_a - C_a}{P_d(B_a+L_a)\nu}. \quad (4)$$

In short, we find a mixed BNE strategy when $\mu > \mu_0$, ((*Attack* with probability p_0 if malicious, *Not attack* if regular), *Defend* with probability q_0 if defensive, *Not defend*if regular). We can also analyse the BNE based on the categories of node B's strategies, and the result is similar.

B. Dynamic Bayesian Game Model

The dynamic Bayesian game model is an extension of static model, where we use repeated game to continually update the belief of both sides about the opponents. The procedure and main components is shown in Fig.3.

Deriving from Bayes rule [13], the update functions of node *A* and *B*'s belief about opponents are

$$\mu(T_a|A_a, H_{a0}) = \frac{\mu(T_a, H_a)P(A_a|T_a, H_{a0})}{\sum_{T_{ai}} \mu(T_{ai}, H_a)P(A_a|T_{ai}, H_{a0})}, \quad (5)$$
$$\nu(T_b|A_b, H_{b0}) = \frac{\nu(T_b, H_b)P(A_b|T_b, H_{b0})}{\sum_{T_{bi}} \nu(T_{bi}, H_b)P(A_b|T_{bi}, H_{b0})}. \quad (6)$$

Here, μ is still expected value of node *A* being malicious; T_a and T_{ai} stand for node *A*'s type (malicious or regular); A_a is the latest action of node *A*; H_a is the game history of node A, $H_a = (A_{a1}, A_{a2}, ..., A_{aN})$ and A_{ai} is node *A*'s action in stage *i*, $1 < i < N$; $P(A_a|T_{ai}, H_{a0})$ represents the probability of node *A* plays action A_a, given the game history and node type. ν is expected value of node *B* being defensive ; T_b and T_{bi} stand for node *B*'s type (defensive or regular); A_b is the

latest action of node B; H_b is the game history of node B, $H_b = (A_{b1}, A_{b2}, ..., A_{bN})$ and A_{bi} is node B's action in stage i; $P(A_b|T_{bi}, H_{b0})$ represents the probability of node B plays action A_b, given the game history and node type. A_{ai}, A_{bi} are generated according to $\mu, \nu, p, q, A_{a(i-1)}$ and $A_{b(i-1)}$.

In each stage, node A and node B update their expectations about their opponents and conditional attack/defense probability, to get the inputs for next stage. The details of the dynamic bayesian game are illustrated in Algorithm 2.

Algorithm 2 Procedure in One Game Stage i

Input:

μ, prior expected value of node A being malicious ;
ν, prior expected value of node B being defensive ;
p, conditional attack probability;
q, conditional defend probability;

Output:

μ', posterior expected value of node A being malicious;
ν', posterior expected value of node B being defensive;

1: Get actions A_a, A_d from $\mu, p, A_{a(i-1)}$ and $\nu, q, A_{b(i-1)}$:
$A_a = (2^{-A_{a(i-1)}} \times rand() < \mu p)$,
$A_d = (2^{-A_{d(i-1)}} \times rand() < \nu q)$.
2: Get updated expection of opponents μ, ν, as iluustrated in *Equation (5), (6)*.
3: Update conditional probability p and q, as iluustrated in *Equation (3), (4)*.

For an improved TBDS, thresholds V_0,k_0 will be automatically adjusted to approach optimal detection strategy. We propose a scheme to continually update V_0,k_0 according to TBDS's payoffs E_D, E_{ND} in *Equation (1)(2)*. In a BNE strategy, we get $E_D - E_{ND} = 0$, while in a no-BNE strategy a larger value of $|E_D - E_{ND}|$ indicates a bigger deviation from BNE. Thus we propose to update V_0 according to $(E_D - E_{ND})$. Since k indicate the variation trend of traffic, we propose to update k_0 according to the variation trend of deviation $((E_D - E_{ND}) - (E'_D - E'_{ND}))$. The detail of adjustment strategy is illustrated in *Equation (7)(8)*.

$$V_0 = V'_0 + \delta_1 \times (E_D - E_{ND}) \quad (7)$$

$$k_0 = k'_0 + \delta_2 \times ((E_D - E_{ND}) - (E'_D - E'_{ND})) \quad (8)$$

V'_0, k'_0 are thresholds in previous game stage; E'_D, E'_{ND} are TBDS's payoffs in previous game stage; δ_1, δ_2 are pre-set fixed parameters, which affect the adjustment speed.

V. Simulations

A. Simulation Settings

We set the number of game stages N = 50 for a balance of accuracy and efficiency. Other parameters are set as follow:

$\mu_0 = \nu_0 = 0.5$,
$p_0 = q_0 = 0.5$,
$B_a = B_d = 100$,
$L_a = L_d = 120$,
$C_a = 10, C_d = 50$,
$t_0 = 1s, M = 50$.

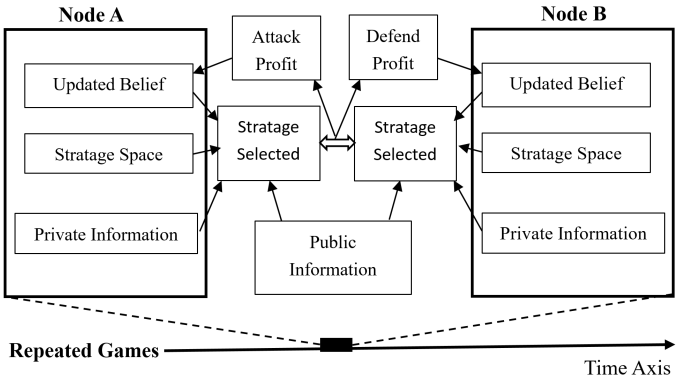
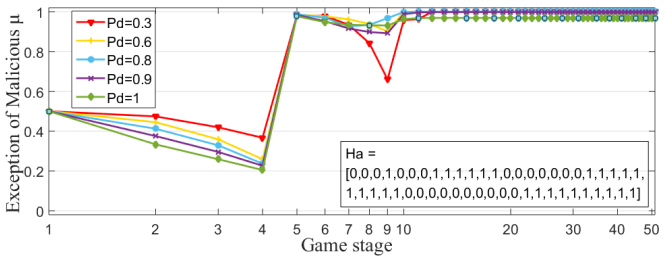
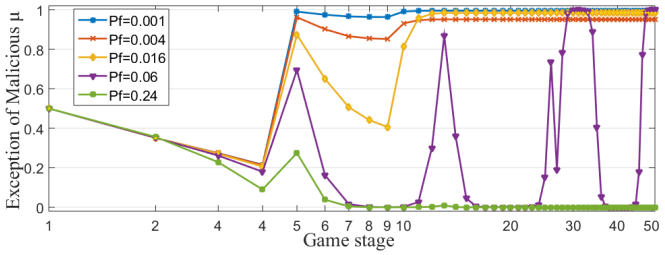


Fig. 3: Procedure of dynamic bayesian game.



(a) True positive rate P_d varies, P_f=0.001



(b) P_d = 0.918, false positive rate P_f varies

Fig. 4: The game process under different P_d and P_f.

Attack history H_a (shown in Fig.4(a)) is generated by belief updating process and behaviour continuity of node A. Action *Attack* is represented by $H_a(i) = 1$, *Not attack* is represented by $H_a(i) = 0$, i represents the index of game stage.

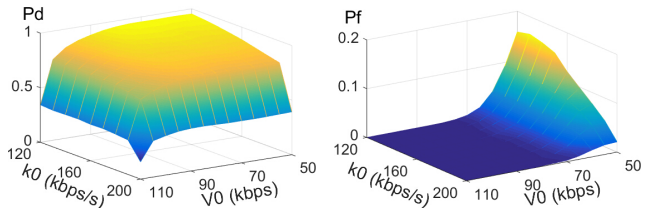
B. Simulation results

According to static Bayesian game, there are two types of equilibrium:

1) When $\mu < \mu_0$, ((*Attack* if malicious, *Not attack* if regular), *Not defend*).
2) When $\mu > \mu_0$, ((*Attack* with probability p_0 if malicious, *Not attack* if regular), (*Defend* with probability q_0 if defensive, *Not defend* if regular))

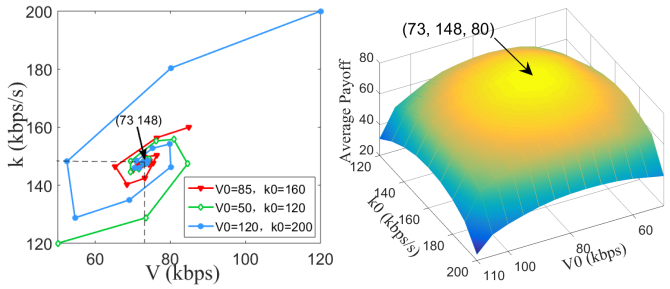
Our simulation describes the second situation. There's no pure BNE when $\mu > \mu_0$, while a mixed BNE is still achievable. In mixed BNE, p and q reduce the actual attack and defense rate to μp and νq. The mixed BNE is also related to P_d and P_f, which are in relation to V_0 and k_0 in TBDS.

The dynamic Bayesian game process is shown in Fig.4. Since fluctuation of μ is extremely small after first ten game



(a) True positive rate (b) False positive rate

Fig. 5: The variation of detection rate and false positive rate when V_0 k_0 change.



(a) Adjustment process of V_0, k_0 (b) Payoffs of node B

Fig. 6: The game process under different P_d and P_f.

stages in most situations, we use logarithmic x axis in Fig.4. There's a high degree of consistency between the curve shape and attack history H_a, as illustrated in Fig.4(a):

1) During the *1st* to *3rd* stages and *5st* to *7th* stages, μ goes down since there's no attack.
2) At the *4th* stage, μ goes up sharply because of an attack.
3) After the *8th* stage, μ converges to 1 since there are several continual attacks. μ won't go down anymore, even if there is a series of no-attack stages.

As illustrated in Fig.4(a), fluctuation of μ increases as P_d decreases. In another word, the higher P_d is, the more stable μ and the faster convergence TBDS can get. Effect of P_f follows the opposite pattern as shown in Fig.4(b). Besides, increment of P_f is more impactive that decline of P_d:

1) When $0 < P_f < 0.02$, μ converges to 0, and a higher P_f results in more severe fluctuation and slower convergence.
2) When $0.02 < P_f < 0.2$, μ fluctuates between 0 and 1, which means there's no convergence. In this case, the TBDS can't distinguish a malicious node reliably.
3) When $P_f > 0.2$, μ converges to 0, which means the detection system totally fails.

As illustrated in Fig.5, selection of P_d and P_f is a tradeoff: increment of P_d will go along with the increment of P_f. The reason is as follow: increment of V_0 increases the deviation between threshold and normal volume $(V_a - V_0)$, resulting in higher P_d; increment of V_0 also decreases the deviation between threshold and attacking volume $(V_a - V_0)$, resulting in higher P_f. The same explanation can be applied to k_0.

Since TBDS aims at maximizing its payoff, we need a balanced combination of V_0, k_0 for higher P_d and lower P_f. As illustrated in Fig.6(a), we simulate a dynamic adjustment process for V_0, k_0. The TBDS starts to detect at different pre-set of V_0, k_0, and converges to the same strategy. The convergence point P_0 $(V_0 = 73(kbps), k_0 = 148(kbps/s))$ describes the optimal strategy, where TBDS gets the maximin payoff. Besides, P_d = 0.918, P_f=0.001 at point P. The curve of dynamic game process under this optimal strategy is marked by '*' in Fig.4(b). Fig.6(b) shows the TBDS's average payoff during the adjustment process of V_0, k_0, where x axis and y axis represent different pre-set start points.

We choose three start points for (V_0, k_0): no-attack point P_n(50, 120), middle point P_m(85, 160) and attack point P_a(120, 200). The curve from P_m approaches the convergence point at the fastest speed and gets the highest payoff, since P_m is the closet to P_0. This give us a guidance on selection of V_0, k_0, at the same time verifies the superiority of our scheme.

VI. Conclusion

The TBDS improves the security of VoLTE network in the case of attackers being rational and incomplete information. By increasing true positive rate and decreasing false positive rate of detection, TBDS gets more accurate information about attacker. The optimal choice of detection thresholds under different scenarios can be obtained by simulation of dynamic game model.

References

[1] Li C Y, Tu G H, Peng C, et al. Insecurity of voice solution volte in LTE mobile networks. Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security. ACM, 2015: 316-327.
[2] Kim H, Kim D, Kwon M, et al. Breaking and fixing volte: Exploiting hidden data channels and mis-implementations. Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security. ACM, 2015: 328-339.
[3] Yousif M, Maaly E, Abu I. QoS Performance Analysis for Voice over LTE 3GPP Mobile Networks. 2016.
[4] Jang W, Kim S K, Oh J H, et al. Session-Based Detection of Signaling DoS on LTE Mobile Networks. Journal of Advances in Computer Networks, 2014, 2(3).
[5] Tu G H, Li C Y, Peng C, et al. How voice call technology poses security threats in 4G LTE networks. Communications and Network Security (CNS), 2015 IEEE Conference on. IEEE, 2015: 442-450.
[6] Poyhonen P. System and method for establishing a session initiation protocol communication session with a mobile terminal: U.S. Patent 8,989,737. 2015.
[7] Liang X, Xiao Y. Game theory for network security. Communications Surveys & Tutorials, IEEE, 2013, 15(1): 472-486.
[8] Manshaei M H, Zhu Q, Alpcan T, et al. Game theory meets network security and privacy. ACM Computing Surveys(CSUR), 2013, 45(3): 25.
[9] Liu Y, Comaniciu C, Man H. A Bayesian game approach for intrusion detection in wireless ad hoc networks. Proceeding from the 2006 workshop on Game theory for communications and networks. ACM, 2006: 4.
[10] Federal Standard 1037C. http://www.its.bldrdoc.gov/fs-1037/fs-1037c.htm.
[11] Camarillo G, Garcia-Martin M A. The 3G IP multimedia subsystem (IMS): merging the Internet and the cellular worlds. John Wiley & Sons, 2007.
[12] Jailani E, Ibrahim M, Rahman R A. LTE speech traffic estimation for network dimensioning. Wireless Technology and Applications (ISWTA), 2012 IEEE Symposium on. IEEE, 2012: 315-320.
[13] Efron B. Bayes theorem in the 21st century. Science, 2013, 340(6137): 1177-1178.