Journal of Zhejiang University SCIENCE A
ISSN 1009-3095 (Print); ISSN 1862-1775 (Online)
www.zju.edu.cn/jzus; www.springerlink.com
E-mail: jzus@zju.edu.cn

Cost management based security framework in mobile ad hoc networks

YANG Rui-jun[†1,2], XIA Qi[1,2], PAN Qun-hua[1], WANG Wei-nong[2], LI Ming-lu[1]

([1]*Department of Computer Science & Engineering, Shanghai Jiao Tong University, Shanghai 200030, China*)

([2]*Network Information Center, Shanghai Jiao Tong University, Shanghai 200030, China*)

[†]E-mail: rjyang@sjtu.edu.cn

Received June 20, 2005; revision accepted Oct. 19, 2005

Abstract: Security issues are always difficult to deal with in mobile ad hoc networks. People seldom studied the costs of those security schemes respectively and for some security methods designed and adopted beforehand, their effects are often investigated one by one. In fact, when facing certain attacks, different methods would respond individually and result in waste of resources. Making use of the cost management idea, we analyze the costs of security measures in mobile ad hoc networks and introduce a security framework based on security mechanisms cost management. Under the framework, the network system's own tasks can be finished in time and the whole network's security costs can be decreased. We discuss the process of security costs computation at each mobile node and in certain nodes groups. To show how to use the proposed security framework in certain applications, we give examples of DoS attacks and costs computation of defense methods. The results showed that more secure environment can be achieved based on the security framework in mobile ad hoc networks.

Key words: Network attacks, Mobile ad hoc, Cost management, Security framework
doi:10.1631/jzus.2006.A0493 **Document code:** A **CLC number:** TP393.08

INTRODUCTION

Mobile ad hoc networks are under active research focused on issues such as routing, security (Venkatraman and Agrawal, 2003) and data management (Fan and Zhang, 2004). People have proposes many kinds of security mechanisms such as SAR (Yi *et al*., 2002), SRP (Papadimitratos and Haas, 2002), ARAN (Sanzgiri *et al*., 2002), ARIADNE (Hu *et al*., 2005) and SEAD (Hu *et al*., 2002) for networks. The resource consumptions of security mechanisms are always large in mobile ad hoc networks so the cost is very high when multiple security methods are combined to resist attacks and prop up system weaknesses. Sometimes resources such as bandwidth, power and media storages are wasted or inefficiently applied. From the viewpoint of the whole ad hoc networks, the total costs of network security should be taken into account besides finishing the networks' main tasks.

There are reasons for the high costs of security mechanisms. First, the own characteristics of mobile ad hoc network account for the main factor. Mobile ad hoc networks are resource limited systems themselves and component mobile nodes have finite usable resources either of power, bandwidth or processing ability and memories though their capacities are determined by certain applications. The restricted resource of each node is a big weakness for mobile ad hoc network. So the cost issues should be considered both in network basic functions design and other appended mechanisms.

The second reason is related with the mechanisms of mobile ad hoc network. At the beginning people did not bring ad hoc network protocols designing into the security problems. And security mechanisms are developed and attached to older protocols when some security leaks and network attacks occur. The new security mechanisms are

added into the network protocols or integrated as a security module. The costs of multiple nodes or multiple mechanisms for united defense again attacks are rarely considered. So the working mechanisms related security costs should be paid more attention.

The assumptions about radio propagations are related to reasons about high security costs. Those security schemes are supposed to help the system to satisfy some security requirements although the results were just obtained through some simulations. Newport (2004) pointed out the simplistic radio models may lead to manifestly wrong results. Akyildiz *et al*.(2005) indicated that theoretical results on the capacity of ad hoc networks are still based on some simplified assumptions. It is simulation's radio propagation assumptions that make things to be different from what they are supposed to be. Those simulations were implemented under nearly perfect assumptions and outcomes may be subverted causing larger costs when they are done in realistic scenarios.

The rest of this paper is organized as follows: in Section II, we discuss the existing security schemes and attacks and present details of security costs in each node and each mechanism. In Section III, we provide a security framework based on cost management and describe the costs computing process at each node or in some nodes groups. The analysis on DoS attacks and defenses under the proposed security framework can be found in Section IV, where some security mechanisms reconfiguration's effects are presented. The last section concludes this paper with a statement about existing issues and future work.

ANALYSIS OF NETWORK ATTACKS AND SECURITY MECHANISMS

The fundamental requirements of computer security like confidentiality, integrity, authentication and non-repudiation are absolutely indispensable when protection of correct network behaviors is to be considered in mobile ad hoc networks. The characteristics of mobile ad hoc networks make them vulnerable to various forms of attacks, which can be classified into different categories according to different standard. Attacks can be classified into passive attacks in which an attacker just eavesdrops on the network traffic to get useful information for future attacks, or active attacks in which an attacker actively participates in disrupting the normal operation of network protocols (Venkatraman and Agrawal, 2003). Attacks can also be classified into internal and external threats. Unauthorized nodes or entities initiating external attacks include passive eavesdropping and active interference. Authorized nodes within the ad hoc network may initiate internal attacks. These threats are thus likely to be more difficult to detect as they arise from trusted sources.

Attacks are always restricted within certain network applications. When facing aggression security mechanisms have to do their best to cope with the problems. It is believable that attacks can occur at almost all layers from one time to another with different styles. For different layers and different types of attacks, some adaptive security frameworks have been proposed which take into account the structures of security networks but have little knowledge on how to induce cooperation among multiple security networks. People facing combined attacks have developed combined security mechanisms to resist them.

When facing security problems occurring at more than two layers simultaneously, single layer protocol cannot deal with them by themselves and so need cooperation by several layers' security mechanisms. But protection against one type of attack may weaken the network against a second type of attack and it is extremely difficult to find the right balance. Another problem is that having two separate protocols at each layer performing similar functions in an uncoordinated manner may lead to large overhead.

From the viewpoint of cross-layer interactions, multidimensional safeguard architecture can be adopted. The many security mechanisms proposed before can be combined according to specific security requirements from the MAC level to application level. Cross layer feedback can be useful in both lower-to-upper direction and upper-to-lower direction in order to reduce the security costs.

Some security mechanisms begin to run before encountering attacks but others startup while suffering attacks. So it is hard to compute the cost of security schemes in mobile ad hoc networks. The total running cost at one node is composed of CPU occupancy factor, power consumption, bandwidth occupancy factor and memory utilization. All of the running costs are network-running expenditures neces-

sary for fulfilling tasks. It is necessary for mobile nodes to quantify the running cost C_i at each node i, which is the weighted sum of four factors' corresponding costs:

$$C_i = \alpha C_{i\text{-CPU}} + \beta C_{i\text{-Memory}} + \delta C_{i\text{-Battery}} + \gamma C_{i\text{-Band}}, \quad (1)$$

where $C_{i\text{-CPU}}$, $C_{i\text{-Battery}}$, $C_{i\text{-Band}}$, $C_{i\text{-Memory}}$ are the corresponding CPU occupancy factor, power consumption, bandwidth occupancy factor and memory utilizations, α, β, δ, γ are the weighted coefficients representing their importance.

Every security mechanism has its own security cost C_{security}. Before implementation of a security mechanism, the running cost of a normal network protocol is $C_{\text{pre-secure-mechanism}}$ and after security mechanism is adopted, the running cost is $C_{\text{post-secure-mechanism}}$, so:

$$C_{\text{security}} = C_{\text{post-secure-mechanism}} - C_{\text{pre-secure-mechanism}}. \quad (2)$$

Once the cross layer security mechanisms can cooperate to resist attacks, their combined cost should be smaller than the sum of every individual security mechanism's cost. There are many algorithms for combined security mechanisms whose total cost is not the simple sum of nodes' C_{security}. We propose an adaptive security framework to deal with complex computations of combined security mechanism cost.

SECURITY FRAMEWORK BASED ON COST MANAGEMENT

There are some cross layer security frameworks for dealing with complex weaknesses and attacks in mobile ad hoc networks. Commonly, security mechanisms do not taken into account the cost of security. Application of cost management yielded several principles in designing security frameworks: (1) The security cost should be lowest in implementing the whole network's security mechanisms. And we should pay attention to the tradeoff between the total benefits of the whole system and the individual node's profit; (2) The cost management should be implemented from the viewpoint of the whole network; (3) Security scheme cost of every layer should be calculated; (4) Cost management should be aimed at getting the greatest security benefits at minimum cost. In order to manage effectively, we should forecast, analyze, calculate and harmonize the security costs among nodes.

When facing threats, the security system can configure its own limited resource according to the feedback results from different stage of cost management. Every node first calculates its own cost, and judges whether it needs support from other nodes. If so, it should collect the involved nodes' costs according to cooperation in the nodes group resisting attacks. After simple calculation, the security system judges and decides how to reconfigure its security mechanisms and then distributes the security tasks among nodes according to predefined principles.

It was found that the following questions should be considered in designing cost management based security framework in order to deal with reasonable collocation of security mechanisms: (1) How to recognize resource wasting and to determine the area of wasting and offer relevant information to nodes or system; (2) The reason for the change of cost should be ascertained. Analysis of the current situation can pinpoint the source of waste; (3) Where the cost analysis is conducted; (4) When the implementations of security mechanism begin to carry out; (5) In which specific node the secure mechanisms are processed. Only by adjusting the security mechanisms at some levels can we develop a new defense protocol.

As shown in Fig.1, we propose a security framework based on cost management. The security framework has four parts. Besides the normal ad hoc network protocols' running module, the security mechanisms' configuration module and reconfiguration module have also important roles in the security costs effects of the whole network. Both of them are centered in the security cost management module. First, some security mechanisms such as security routing protocol authorization and authentication should be set in the network nodes in order to prevent some known attacks. Some attacks may be found while the network is running and so relevant security schemes must be adopted to resist them. Before their working, we should compute the costs budgets of security measures and repeat the same computation a second time after somewhile or after completing se-

curity schemes running. These processes are executed more times when facing large scale attacks. The changes between the budgets and real costs can be fed back and used for analysis of security mechanisms reconfigurations. At the same time, resistant nodes or nodes groups can use the feedback information to evaluate the whole effectiveness of costs and reconfigure the security mechanisms if necessary.

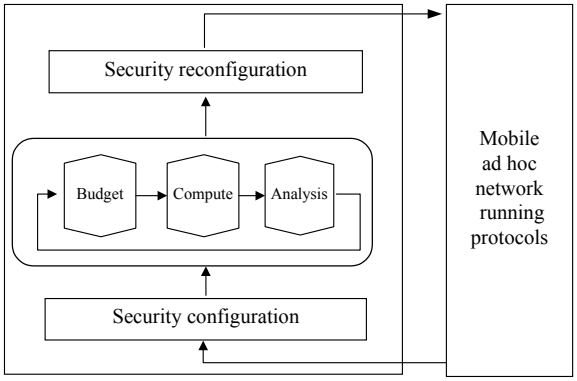

Fig.1 Cost management based secure framework

The flow of costs computation in the security framework is shown below.

Single node security costs computation

The nodes in the whole network, the corresponding network operating costs from application, transport, network, to MAC and physical layer, are shown in Table 1.

As mentioned in a former section, the normal running cost of each mobile node is shown in Eq.(1). Every layer's running costs are $C_{i\mathrm{A}}$, $C_{i\mathrm{T}}$, $C_{i\mathrm{N}}$, $C_{i\mathrm{M}}$, $C_{i\mathrm{P}}$, which can be computed according to:

$$C_{i\psi}=\alpha_{\psi}C_{i\psi\text{-CPU}}+\beta_{\psi}C_{i\psi\text{-Memmory}}+\delta_{\psi}C_{i\psi\text{-Battery}}+\gamma_{\psi}C_{i\psi\text{-Band}}, \tag{3}$$

ψ means certain layer. The computed $C_{i\mathrm{A}}$, $C_{i\mathrm{T}}$, $C_{i\mathrm{N}}$, $C_{i\mathrm{M}}$, $C_{i\mathrm{P}}$ are stored in vector $\boldsymbol{V}_{C_i}$:

$$\boldsymbol{V}_{C_i}=(C_{i\mathrm{A}}, C_{i\mathrm{T}}, C_{i\mathrm{N}}, C_{i\mathrm{M}}, C_{i\mathrm{P}}). \tag{4}$$

As mentioned above, every security mechanism's cost is shown in Eq.(2).

For certain layer security mechanism, the costs $C_{i\mathrm{A}}$, $C_{i\mathrm{T}}$, $C_{i\mathrm{N}}$, $C_{i\mathrm{M}}$, $C_{i\mathrm{P}}$ always change after adopting of a security mechanism. And they can be computed as:

Table 1 Normal running cost of each layer protocol

I	A	T	N	M	P	
1	$C_{1\mathrm{A}}$	$C_{1\mathrm{T}}$	$C_{1\mathrm{N}}$	$C_{1\mathrm{M}}$	$C_{1\mathrm{P}}$	
2	$C_{2\mathrm{A}}$	$C_{2\mathrm{T}}$	$C_{2\mathrm{N}}$	$C_{2\mathrm{M}}$	$C_{2\mathrm{P}}$	
3	$C_{3\mathrm{A}}$	$C_{3\mathrm{T}}$	$C_{3\mathrm{N}}$	$C_{3\mathrm{M}}$	$C_{3\mathrm{P}}$	
⋮	⋮	⋮	⋮	⋮	⋮	…
i	$C_{i\mathrm{A}}$	$C_{i\mathrm{T}}$	$C_{i\mathrm{N}}$	$C_{i\mathrm{M}}$	$C_{i\mathrm{P}}$	
⋮	⋮	⋮	⋮	⋮	⋮	
n	$C_{n\mathrm{A}}$	$C_{n\mathrm{T}}$	$C_{n\mathrm{N}}$	$C_{n\mathrm{M}}$	$C_{n\mathrm{P}}$	

I: node; A: application; T: transfer; N: network; M: MAC; P: physical

$$C_{i\psi\text{-security}}=C_{i\psi\text{-post-secure-mechanism}}-C_{i\psi\text{-pre-secure-mechanism}}, \tag{5}$$

ψ indicates some layer of the network protocol.

Security weaknesses occur indeterminably in some layers and we use one vector to distinguish the security related costs change from the change due to normal system running when computing the security mechanisms costs.

$$\boldsymbol{V}_{O_i}=(o_{i\mathrm{A}},o_{i\mathrm{T}},o_{i\mathrm{N}},o_{i\mathrm{M}},o_{i\mathrm{P}}),\quad o_{ik},\ k\in\{\mathrm{A,T,N,M,P}\}. \tag{6}$$

The values of $o_{i\mathrm{A}}$, $o_{i\mathrm{T}}$, $o_{i\mathrm{N}}$, $o_{i\mathrm{M}}$, $o_{i\mathrm{P}}$ can only be 0 or 1 respectively representing whether security schemes are adopted or not. If not, the results in each of the factors should not be included in $C_{i\psi\text{-security}}$. That is to say, for node i, its security cost can be computed though the non-zero values in the vector $\boldsymbol{V}_{CO_i}$:

$$\begin{aligned}\boldsymbol{V}_{CO_i}&=\boldsymbol{V}_{C_i}\times\boldsymbol{V}_{O_i}\\&=(C_{i\mathrm{A}}, C_{i\mathrm{T}}, C_{i\mathrm{N}}, C_{i\mathrm{M}}, C_{i\mathrm{P}})\times(o_{i\mathrm{A}}, o_{i\mathrm{T}}, o_{i\mathrm{N}}, o_{i\mathrm{M}}, o_{i\mathrm{P}}).\end{aligned} \tag{7}$$

The values of $\boldsymbol{V}_{O_i}$ can be re-written by its set defense node. The whole costs of one node is

$$C_{i\text{-security}}=\sum C_{i\phi}o_{i\phi}, \tag{8}$$

where ϕ represents the layer in which the value of $C_{i\phi}o_{i\phi}$ is nonzero.

When the node computes its own costs, it can also calculate the costs ratio:

$$\eta_i = C_{i\text{-security}}/C_i = \sum C_{i\phi} o_{i\phi} \Big/ (C_{i\mathrm{A}} + C_{i\mathrm{T}} + C_{i\mathrm{N}} + C_{i\mathrm{M}} + C_{i\mathrm{P}}). \quad (9)$$

The ratio indicates the secure mechanisms costs proportion to the whole running costs.

Local group cost computation

During every small period, some nodes can be made up of one group in some small area. The principal node, which has largest usable resource, is charged with computing the local group costs.

1. Selection of the principal node

When one node has the largest resource to use compared with neighboring nodes, it can be used for computing the group cost. In order for the principal node to make a correct choice, the neighboring nodes must exchange their information on usable resource.

2. Setup for size of group and computing period

When the network is running, the local group cost should be computed periodically. Once a node completes computation of its own first time security cost computing, it can send indication about its attempt to compute local group cost. When more than half of several adjacent nodes sense the attempts from each other they can select the principal node and begin the first-time group cost computation. The principal node only includes those nodes inside one-hop in its current group. After group cost calculation, the principal node feeds back some cost information to its group's nodes. In order that some nodes compute the group cost at the same time, one node cannot take part in another group cost computation when it is already participating in one computation.

3. Local groups cost computation

The principal node requires nodes in its group to send their own security costs and computes the group costs:

$$C_{\text{Group}} = \sum C_{i\text{-security}}. \quad (10)$$

At the same time, it can also calculate the group security costs ratio used in future security analysis. Here m is the number of nodes in the group.

$$\eta_{\text{Group}} = \sum_{i=1}^{m} C_{i\text{-security}} \Big/ \sum_{i=1}^{m} C_i = \sum_{i=1}^{m} \sum C_{i\phi} o_{i\phi} \Big/ \sum_{i=1}^{m} (C_{i\mathrm{A}} + C_{i\mathrm{T}} + C_{i\mathrm{N}} + C_{i\mathrm{M}} + C_{i\mathrm{P}}). \quad (11)$$

It is hard to share security information so the global security costs and cooperation among nodes become too difficult to implement. Some models should be proposed to predict the execution time of a single job or multiple jobs on each mobile node with varied security mechanisms costs. Gao *et al*.(2003) presented an approach to scheduling jobs on a service grid using genetic algorithm (GA). We will do some further work based on this method.

Security cost computation in larger area

During every large period, former principals can set up a large-scale security cost computation in larger area. Due to the mobility of nodes it is too hard to compute global security costs. We can just calculate the security cost of nodes in larger area. The tasks are still charged by principals who need nodes to store some local security costs and cost ratios and to exchange them among these nodes.

These principal nodes should send indications to the same type of nodes besides two-hop about their intension to calculate security costs in larger area. These proposals only can be accepted and calculated instantly to provide the involved groups' security association with the system global cost.

The computing method is similar to that of above steps but only two types of parameters are used here. For example, node B receives two local security cost related parameter values $\eta_{\text{Group-}A}$ and $C_{\text{Group-}A}$ from node A (here $C_{\text{Group-}A} = \sum C_{i\text{-security}}$, $i \in \text{Group-}A$) and combines them with its parameters $\eta_{\text{Group-}B}$ and $C_{\text{Group-}B}$. Then it can calculate the security association $\phi_{\text{Group-}A,\text{ Group-B}}$ in larger area around link A-B:

$$\phi_{\text{Group-}A,\text{Group-}B} = (C_{\text{Group-}A} + C_{\text{Group-}B}) / [(C_{\text{Group-}A} / \eta_{\text{Group-}A}) + (C_{\text{Group-}B} / \eta_{\text{Group-}B})]. \quad (12)$$

Here we only implement simple cost management and the approximate global security costs can be obtained through several larger areas security cost computations.

Under this security framework, there are certainly some difference between the pre-assigned se-

curity mechanisms costs computations and real costs. The forecasted security costs are:

$$\boldsymbol{C}_{\text{budget}}=\begin{bmatrix}1 & C_{1\text{A-sb}} & C_{1\text{T-sb}} & C_{1\text{N-sb}} & C_{1\text{M-sb}} & C_{1\text{P-sb}}\\ 2 & C_{2\text{A-sb}} & C_{2\text{T-sb}} & C_{2\text{N-sb}} & C_{2\text{M-sb}} & C_{2\text{P-sb}}\\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots\\ m & C_{m\text{A-sb}} & C_{m\text{T-sb}} & C_{m\text{N-sb}} & C_{m\text{M-sb}} & C_{m\text{P-sb}}\end{bmatrix} \quad (13)$$

where sb means security-budget.

And the real costs of security mechanisms are:

$$\boldsymbol{C}_{\text{reality}}=\begin{bmatrix}1 & C_{1\text{A-sr}} & C_{1\text{T-sr}} & C_{1\text{N-sr}} & C_{1\text{M-sr}} & C_{1\text{P-sr}}\\ 2 & C_{2\text{A-sr}} & C_{2\text{T-sr}} & C_{2\text{N-sr}} & C_{2\text{M-sr}} & C_{2\text{P-sr}}\\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots\\ m & C_{m\text{A-sr}} & C_{m\text{T-sr}} & C_{m\text{N-sr}} & C_{m\text{M-sr}} & C_{m\text{P-sr}}\end{bmatrix} \quad (14)$$

where sr means security-reality.

The changes are:

$$\boldsymbol{C}_{\text{variety}}=\boldsymbol{C}_{\text{reality}}-\boldsymbol{C}_{\text{budget}} \quad (15)$$

Because the mobile nodes keep moving and the nodes group keep changing, we can only remind of the system security conditions through checking the security cost ratios and security costs in short periods. The system at each mobile node can operate its own vector $\boldsymbol{V}_{O_i}$ and modify its elements' values to configure the security mechanisms. The network can re-assign the whole system's security strategy according to the matrix:

$$\boldsymbol{O}_{\text{re-secure-conf}}=\begin{pmatrix}1 & O_{1\text{A}} & O_{1\text{T}} & O_{1\text{N}} & O_{1\text{M}} & O_{1\text{P}}\\ 2 & O_{2\text{A}} & O_{2\text{T}} & O_{2\text{N}} & O_{2\text{M}} & O_{2\text{P}}\\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots\\ m & O_{m\text{A}} & O_{m\text{T}} & O_{m\text{N}} & O_{m\text{M}} & O_{m\text{P}}\end{pmatrix} \quad (16)$$

Here the values ($o_{i\text{A}}$, $o_{i\text{T}}$, $o_{i\text{N}}$, $o_{i\text{M}}$, $o_{i\text{P}}$) of $\boldsymbol{V}_{O_i}$ could be re-written by involved nodes.

EXAMPLE OF SECURITY CONFIGURATION UNDER SECURITY FRAMEWORK

In the implementation of the proposed security framework, each node has to be charged with its own tasks when facing attacks. Here we exemplify the DoS attacks and protections as shown by our cost management based security framework. DoS attacks aim to prevent access to network resources and can be devastating and difficult to protect against. It can target different layers and there is much difference between various types of DoS attacks. Traffic patterns generated by an attacking node, its location in the network, availability of other compromised nodes and routing information are key factors in determining the efficacy of the DoS (Aad *et al*., 2004).

Here we conduct some tests on cost management for DoS attacks and defenses based on the proposed security framework. The main objective is to improve the effectiveness of security mechanisms cost either for single mobile node or for the mobile nodes group.

As shown in Fig.2, suppose an ad hoc network contains twenty nodes numbered from 1 to 20 and three attack nodes named *A*1, *A*2, and *A*3. Nodes around the attack nodes randomly organize three nodes groups. It will set up two big local security conjunctions between nodes 3 and 11 as well nodes 11 and 17. First we calculate every security cost of the twenty nodes marked as C_1, C_2, …, C_{20}. Then, we compute the group costs of Group1, Group2, Group3 and proportion of security cost to whole running cost η_{Group1}, η_{Group2}, η_{Group3}, centered around nodes 2, 11 and17 responsible for the computing tasks. At last, the security association $\phi_{\text{Group1,Group3}}$ between nodes 1 and 11 as well as $\phi_{\text{Group2,Group3}}$ between nodes 11 and 17 are figured out.

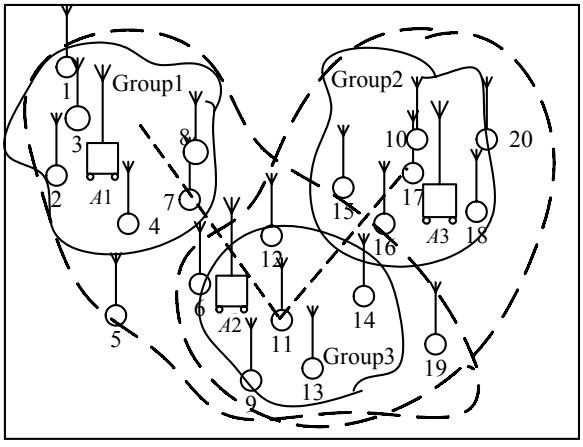

Fig.2 Scenario exemplifying DoS attacks and defenses

We consider the configuration of the security schemes in the security framework from several aspects: If the system detected attacks and defense actions are deployed, the costs of security will turn larger. At this time, the system should estimate the invalid costs. For the residual resources there are three kinds of scenarios including satisfying the requirements of system running, completing parts of mission ineffectively, and losing basic functions. For each instance we should adjust the costs in time.

These data can be used to collocate the security scheme of the nodes in the group. For example, at some time in Group1, the attacker $A1$ sends exhaustion attack to node 1, the node 1 prefabricates small frames security scheme, while the nodes 2 and 4 startup client puzzles security scheme to counter the flooding attack from $A1$. If $A1$ makes misdirection to nodes 7 and 8, which we assume the two nodes have prefabricated authorization. Because the node 3 has not been attacked from $A1$, it has so many sources to use to startup the security cost calculation of Group1. It can notify every node to relocate the security mechanisms by calculating every node's security cost and ratio. Through simulating the security mechanisms reconfiguring of the nodes in Group1, we get some graphs of CPU and band utilization ratio as shown in Fig.3 in which the y-axis indicates the utilization ratio of CPU and network bandwidth and x-axis indicates the time used in simulation.

The occupancy factor of CPU of node 3 is small at the beginning. It increases after starting up the calculation of the costs. At first, the band is transferring the data normally. When the other nodes are attacked, it has less data to transfer with them so that its band is decreased. Because the nodes 7 and 8 have prefabricated security schemes, their bands and CPUs are changing when attacked. And then, they can resist the attacks through their own security schemes, with the result that the curve in the graph changes smoothly.

The band of node 1 when attacked is stable at first but keeps a low bandwidth-utilizing ratio, so it could not be adjusted. But because it uses small frames, its occupancy factor of CPU was high. We can modify this through its security scheme to decrease its CPU occupancy factor. Nodes 2 and 4 have the same conditions when facing flooding attacks, because they adapt the client puzzle methods, the CPU keeps working at high occupancy factor and the bandwidth utilization are also too large. At this time, the security costs become too abnormally high and the system running is affected badly. We should not care about some attacks and mitigate the CPU's overload sacrificing bandwidth, which can satisfy the basic data transferring requirements though sill keeping the relatively high CPU overload.

The above figures tell us that the local group's security costs can be used to enhance the effects of security costs and to improve the availabilities of nodes in larger areas in the mobile ad hoc networks. For more complex applications and implementations of security framework such as costs computation of whole networks nodes and scalability of cost management framework, we still keep on studying and in the future may introduce some QoS's evaluating methods to detect the effectiveness of security mechanisms reconfigurations schemes under this security framework.

CONCLUSION AND FUTURE WORK

In this paper we detailedly investigated network attacks and security mechanisms and proposed a security framework based on cost management. After presenting the implementation of costs computation, we exemplify DoS attacks and defenses based on cost management and maintain that most security mechanisms configurations can be done under the proposed security framework. The results showed that the mobile ad hoc network shortcoming of node's limited resources can be overcome to some extent and that the effects of security costs can be improved with increasing availability of ad hoc networks in more realistic scenarios.

There are some problems left for us to work on in the future. The weighted coefficients in the weighted sum of every layer security mechanisms costs are hard to choose suitably. It should be accommodated to certain application security requirements and now we give them values by our experiences. It should be determined self-adaptively in the future. It is difficult to calculate the costs of cross layers security mechanisms for some counteracts in co-operations and the modularization of each security mechanism costs computing should be considered under our proposed security framework.

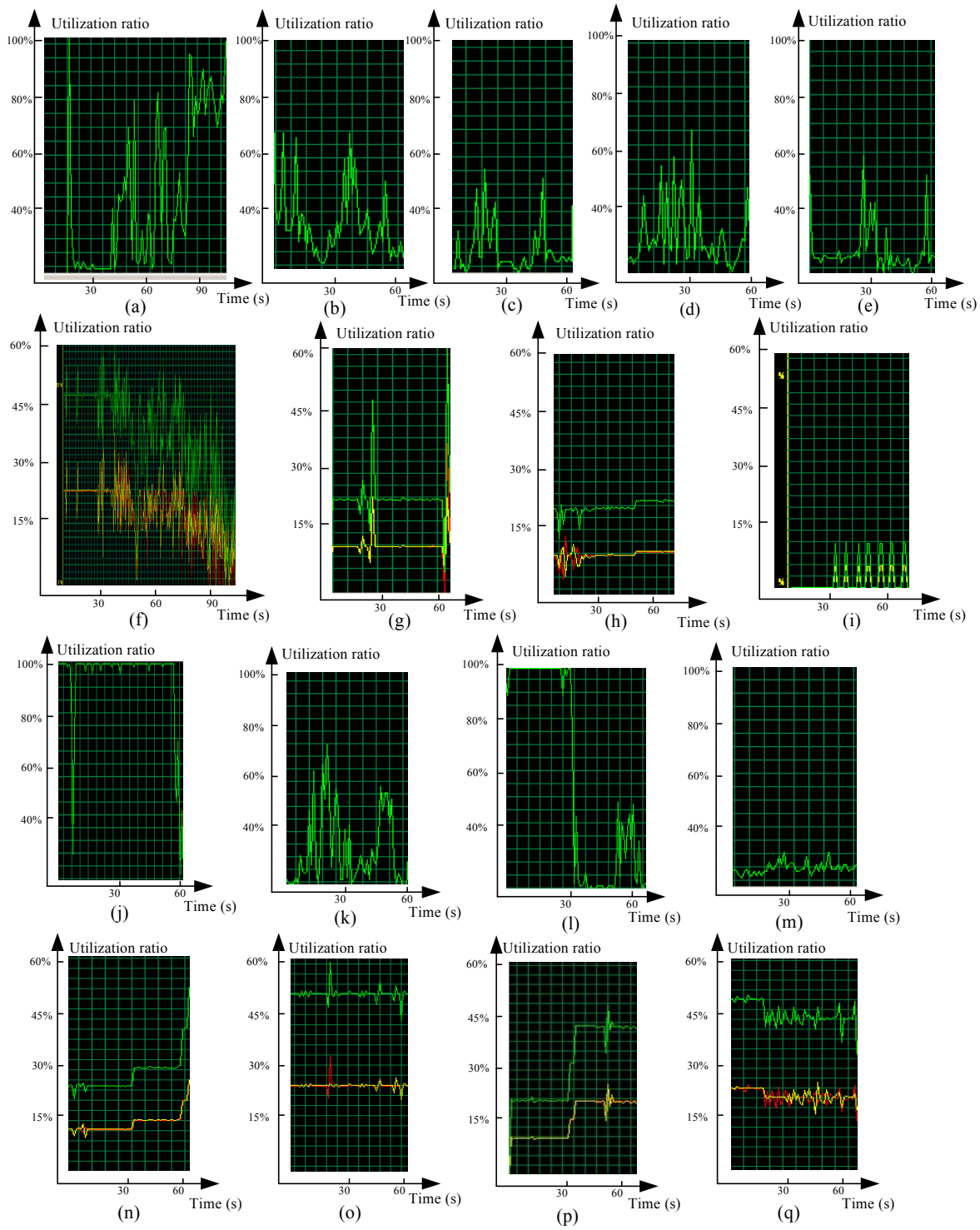

Fig.3 CPU and band utilization ratio variation curves of nodes in simulation

(a) Node 3's CPU variation curve; (b) Node 7's CPU variation curve; (c) Node 8's CPU variation curve; (d) Node 1's CPU variation curve after configuration-1; (e) Node 1's CPU variation curve after configuration-2; (f) Node 3's Bandwidth variation curve; (g) Node 7's Bandwidth variation curve; (h) Node 8's Bandwidth variation curve; (i) Node 1's Bandwidth variation curve; (j) Node 2's CPU variation curve after configuration-1; (k) Node 2's CPU variation curve after configuration-2; (l) Node 4's CPU variation curve after configuration-1; (m) Node 4's CPU variation curve after configuration-2; (n) Node 2's Bandwidth variation curve after configuration-1; (o) Node 2's Bandwidth variation curve after configuration-2; (p) Node 4's Bandwidth variation curve after configuration-1; (q) Node 4's Bandwidth variation curve after configuration-2

References

Aad, I., Hubaux, J.P., Knightly, E.W., 2004. Denial of Service Resilience in Ad Hoc Networks. MobiCom'04, Sept. 26~Oct. 1, 2004, Philadelphia, Pennsylvania, USA, p.43-57.

Akyildiz, I.F., Wang, X.D., Wang, W.L., 2005. Wireless mesh networks: a survey. *Computer Networks*, **47**(4):445-487. [doi:10.1016/j.comnet.2005.01.002]

Fan, G., Zhang, J., 2004. Maximizing sensor reuse based on new geometric concepts. *Journal of Information Science and Engineering (JISE), Special Issue of Mobile Computing*, **20**:477-489.

Gao, Y, Rong, H., Tong, F., Luo, Z., Huang, J., 2003. Adaptive job scheduling for a service grid using a genetic algorithm. *GCC*, (2):65-72.

Hu, Y., Johnson, D., Perrig, A., 2002. SEAD: Secure Efficient Distance Vector Routing for Mobile Wireless Ad Hoc Networks. Proceedings of the 4th IEEE (WMCSA), IEEE, Calicoon, NY, p.3-13.

Hu, Y., Perrig, A., Johnson, D., 2005. ARIADNE: a secure on demand routing protocol for ad hoc networks. *Wireless Networks*, **11**(1-2):21-38. [doi:10.1007/s11276-004-4744-y]

Newport, C., 2004. Simulating Mobile Ad Hoc Networks: A Quantitative Evaluation of Common MANET Simulation Models. Dartmouth College Computer Science Technical Report, TR2004-504.

Papadimitratos, P., Haas, Z.J., 2002. Secure Routing for Mobile Ad Hoc Networks. Proceedings from the SCS Communication Networks and Distributed Systems Modeling and Simulation Conference, p.27-31.

Sanzgiri, K., Dahill, B., Levine, B.N., Belding-Royer, E.M., 2002. A Secure Routing Protocol for Ad Hoc Networks. Proceedings of the 10th IEEE International Conference on Network Protocols (ICNP), Paris, France, p.78-89.

Venkatraman, L., Agrawal, D.P., 2003. Strategies for enhancing routing security in protocols for mobile ad hoc networks. *J. Parallel Distributed Computing*, **63**(2): 214-227. [doi:10.1016/S0743-7315(02)00065-5]

Yi, S., Naldurg, P., Kravets, R., 2002. A Security-aware Ad Hoc Routing Protocol for Wireless Networks. The 6th World Multi-Conference on Systemic, Cybernetics and Informatics (SCI 2002), Orlando, Florida.