Proceedings of APCC2008 copyright © 2008 IEICE 08 SB 0083

TSIPN: Trust-based Resilient Scheme for IP Networks

Junjie Ji, Xiaolong Yang, Jin Wang, Xiongbiao Wu, Jianren Lin, Keping Long, *Senior Member IEEE*

Abstract—**Nowadays, IP networks are suffering many faults and malicious attacks, which greatly threaten its security and survivability. So it is an important issue that how to make the IP networks to be more resilient under faults and attacks, i.e., to improve their tolerance abilities for both fault and intrusion. However recently, most of the researches focus on only one of them, and decouple the survivability and security each other. According to the trust model in social networks, this paper proposes an efficient scheme which is resilient to both fault and intrusion based on trust relationship for IP networks. This scheme not only borrows the trust rating from the social links, but also qualitatively describes the relationships between the trust rating and the network behavior. Then, this paper analyses the scheme how to tolerate three known malicious behaviors, viz., self-faults, bad mouth attacks and conflict behavior attacks. Finally, our scheme can detect the malicious nodes fast and accurately and efficiently prevent these malicious behaviors in IP networks.**

Index Terms—**fault-tolerant, intrusion-tolerant, IP networks, resilient, trust-based**

I. Introduction

THE IP networks are suffering all kinds of misbehaviors including self-faults and malicious attacks, and these misbehaviors become more and more serious. So it is an important issue that how to make the IP networks to be more robust under faults and attacks, i.e., to improve their tolerance abilities for both fault and intrusion. However recently, most of the researches focus on only one of them, and decouple the survivability and security. For example, the self-healing and recovery (e.g.,[8][9][10]) mechanisms enhance the networks' survivability and security by the way of fault-tolerance only in the case of node break down; while traditional cryptographic mechanism (e.g.,[11][12]) and intrusion detection system (e.g.,[13]) by the method of intrusion-tolerance only. The general methods by fault-tolerant or intrusion-tolerant only are shown in Fig. 1 and Fig. 2. So, how to make the networks both fault-tolerant and intrusion-tolerant becomes a valuable issue to study.

All authors are with Research Center for Optical Internet and Mobile Information Networks (COIMIN), Univ. of Electronic Science and Technology of China (UESTC), Chengdu, P.R. China, 610054 (corresponding author to provide phone: +86 028-83207895. e-mails are listed below: jijunjie@uestc.edu.cn, yxl@uestc.edu.cn).

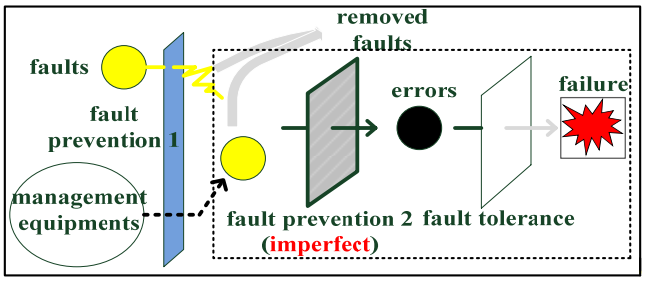


Fig. 1 The resilience from the view of fault only

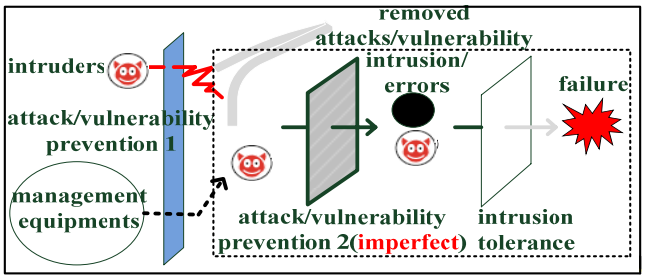


Fig. 2 The resilience from the view of intrusion only

As we know, in social networks, communications between different individuals are based on the trust of each other. In order to contact with somebody, one must have certain credit in the object. Otherwise, its contact will be refused. Accordingly, if one individual has poor reputation, its opinions are doubted or even rejected by others. Above all, we find that IP networks and social networks are very similar on some aspects. So, we use the social trust relationships to construct our IP networks which with the abilities of fault-tolerance and intrusion-tolerance. The use of trust scheme in making the networks both fault-tolerance and intrusion-tolerance is shown in Fig. 3.

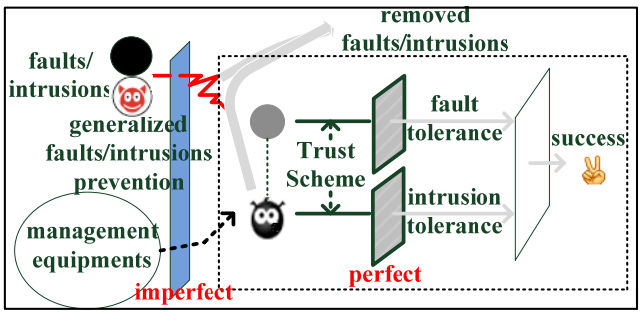


Fig. 3 The resilience from both fault-tolerance and intrusion-tolerance

Therefore recently, some similar trust models are used in communication networks in order to improve their survivability. For example, P. Resnick et al. [1] proposed a centralized reputation system, in which every entity can easily query the trust rating of the other's from a central node. However, the central node can be a bottleneck for accessing the trust rating table due to a single point of failure and poor scalability. CONFIDANT [2] is a routing protocol in Mobile Ad hoc Networks (MANETs) which is a distributed, symmetric reputation system using both first-hand and second-hand trust information for updating trusting values. However, it cannot avoid bad-mouth attacks if we use second-hand information. RFSN [3] is the first reputation and trust-based system designed and developed specially for sensor networks. It uses watchdog mechanism to provide trust rating. However, there is uncertainty in the trust system, because the watchdog cannot record all the behavior due to its own faults. DRBTS [4] is a distributed model using first-hand and second-hand trust information, while lacking deeper and more concrete studies. ATSN [5] is an agent-based trust model in sensor networks. It uses watchdog mechanism to monitor the behavior of other sensor nodes and uses the agent to compute and broadcast the trust values. The sensor node receives the trust value and then makes decision of the behavior of the node which the trust value belongs to. However, on the one hand, it doesn't fully share trust values; on the other hand, it doesn't avoid triangle routing arising by the agent. Also, the method of agent leads to extra cost.

There has some achievements to improve the abilities of fault-tolerance and intrusion-tolerance of networks with the use of trust scheme, but it is still in an entry-level stage. On the one hand, their abilities of fault-tolerance and intrusion-tolerance of networks are not perfect enough, such as poor scalability and less diversity. On the other hand, they can not suit for all kinds of networks. This paper puts forward an efficient fault-tolerant and intrusion-tolerant scheme which formulates the fault events and malicious behaviors of a network node in a trust relationship scheme. Based on the scheme, each node can cooperatively make a decision for the communication action with other nodes regardless of the faults or intrusions.

The main contributions of this paper are as follows. Firstly, it designs a distributed trust-based resilient scheme. Then, it gives the definition, updating and propagation of the trust value in general IP networks. At last, it analyzes the performance of the scheme by simulations on the circumstances of some abnormities in IP networks.

The rest of this paper is organized as follows. We start with a description of the fault-aware and intrusion-aware trust scheme in section Ⅱ. Section Ⅲ depicts the implementation of this scheme. Section Ⅳ presents some misbehavior in IP networks and analyzes our scheme against them. Section Ⅴ, the simulation results are shown. The conclusions are drawn in Section Ⅵ. In the end are the acknowledgements and references.

II. FAULT-AWARE AND INTRUSION-AWARE SCHEME BASED ON TRUST RELATIONSHIP

The fault-aware and intrusion-aware scheme consists of network data collecting, the trust rating computing, the storage and propagation of the trust rating. The flow chart of this scheme is shown in Fig. 5. In the following parts, we will illustrate this scheme in details.

A. Definition and Measurement for Trust Value

T_{ij} is the trust-value that node *i* maintained for node *j*. The trust value is inferred from two parts, one is monitoring the object node directly, which is called direct trust value, the other is referring the neighboring nodes*' opinions, and we call it indirect trust value. So the definition of T_{ij} is as follows:

$$T_{ij} = a(T_{ij})_D + (1-a)(T_{ij})_{ID} \quad (1)$$

Let $(T_{ij})_D$ and $(T_{ij})_{ID}$ be the direct and indirect trust value respectively. $0 \le T_{ij} \le 1, \alpha \in [0,1]$ and can be modified easily by customers in order to differentiate the weights in contribution to the trust value. Generally, we initialize the trust value to 0.5.

The direct trust value is up to the users' requirement on certain application. Different application has different requirement. For example, the telephone desires low delay, the Email requires low loss-rate etc. This scheme permits users to customize the direct trust value.

$$(T_{ij})_D = c_1 f_1(\cdot) + c_2 f_2(\cdot) + \cdots + c_m f_m(\cdot) + \cdots + (1 - c_1 - c_2 - \cdots - c_{n-1}) f_n(\cdot) \quad (2)$$

Here, we suppose that $c_1 + c_2 + \cdots + c_n = 1$,$c_m \in [0,1]$ is constant and can be customized by customers according to the $f_m(.)$' contribution to the trust value. $f_m(.)$ presents the *m*th function for trust mapping. *n* is the number of $f_m(.)$.

The indirect trust value $(T_{ij})_{ID}$ is obtained from the neighboring nodes. However, some neighboring nodes have high trust rate in the source node, other nodes have low trust rate. Then, we should treat the neighboring nodes' opinions differently. The definition is as follows:

$$(T_{ij})_{ID} = \frac{1}{N_i} \sum_{l=1}^{l=N_i} w_{il} * T_{lj} \quad (3)$$

Here, N_i, terms as the number of node *i*'s neighbors. w_{il} is the weight determined by the trust metric T_{il}, and can be derived as follows:

$$w_{il} = \begin{cases} constant, \forall T_{il} \ge TH \\ \frac{1}{2^k} + \frac{1}{2^t}, \forall T_{il} < TH \end{cases} \quad (4)$$

Here, $l \in N_i$. Now, we consider two nodes *i* and *l*. If T_{il} is larger than certain customized threshold TH, then we can deem node *i* cooperative with node *l* and vice versa. In definition (4), *constant* is denoted as the weight about the node *l* when the relation between nodes *i* and *l* is cooperative. We suppose *constant* be "1". $\frac{1}{2^k} + \frac{1}{2^t}$ represents the weight about the node *l* when the relation between nodes *i* and node *l* is uncooperative.

From Definition (4), we can see that the dynamic function has

* In this paper, all the nodes are denotes as routing nodes.

two parameters *k* and *t*. *k* represents the degree of the node, viz., the number of the branches of a node. *t* is a timer. In RFSN [3], nodes just receive the indirect trust value of nodes which are cooperative. In fact, the indirect trust value still could make sense even on the conditions of self-faults or intrusions. So we take the indirect trust value into account no matter the condition is cooperative or not (or "good or bad"), only to make the weights differently on computing the trust value. Then we can share the trust value, yet not on the cost of security.

We distinguish the weight in three ways in Definition (4). Firstly, the node is good or bad. Secondly, the availability of the indirect trust value on the condition of faults or intrusions. Thirdly, it takes the degree of the node into consideration.

B. An Adaptive Update and Binding Propagation of the Trust Value

In this scheme, the trust value is updated in real time. The details of the update scheme are as follows. It takes the direct trust value as the final trust value once the direct trust value beyond the threshold which customized by customers and can content customers' need, ignoring any other indirect trust values. Because the direct trust value is more important and truthful than indirect trust values. Therefore, it not only consumes less computing resources but also improves the efficiency. However, when the direct trust value is below the threshold we still update the trust value according to the Definition (1).

Moreover, we process the indirect trust values before putting in use in Definition (1) in order to enhance the security. With a new defined threshold, it compares the indirect trust value with the average of all the other indirect trust values; if the difference is more than the threshold it will take the indirect trust value as fake information and ignore it. But, if there are *N* nodes' indirect trust values, it will have to compute the averages for *N* times. Amazingly, the degree of most nodes in IP networks is very small [6]. So it will not consume too much computing cost for computing the averages.

In this scheme, each node maintains a table consisting of the routing information and the trust values of the neighboring nodes, which can be called enhanced routing table. The trust value field can be attached behind the general routing information fields. The trust information and the general routing information are bind and propagate together by the enhanced routing protocol.

In this scheme, the trust information and routing information are stored and propagated as a whole. Besides, not only can it use the routine routing storage and propagation strategies but also make the general routers' functions be increased without too much cost. Here, we assume that any routing node maintains the neighboring nodes' trust information only. Also, we do not take the more than one hop's propagation into consideration for simplicity.

III. Implementation of this Scheme

This scheme can be implemented as follows. Node works in a promiscuous mode to collect trust information, and then compute the direct trust value $(T_{ij})_D$ according to Definition (2). According to T_{ij}, the node *i* can decide how to process the behavior between *i* and *j*. Also, the node *i* propagates the value T_{ij} to other nodes as an indirect trust value with the enhanced routing protocol. Fig. 4 depicts the building blocks of this scheme.

Besides, in fact, we can also broadcast the trust information separately without the enhanced routing protocol. But it will cost some extra network loads. So, this paper utilizes the enhanced routing protocol.

The function of promiscuous mode listing and data collecting has been presented at the beginning of section III. The monitoring mechanism is to monitor the behaviors of the neighboring nodes and compute the direct trust value. The direct trust value is gained from Definition (2) in which the functions for trust mapping are customized by customers. For example, we assume the first function to be Packet Delivery Ratio, the second function about time delay, the third one to be the throughput and so on. Customers can customize the types, the number and the concrete form of the functions for trust mapping. Also, we can adjust the weights, just as c_i, in Definition (2). Of course, if c_i equals 0, it suggests that the according function is not chosen. The implementation of monitoring and computing for direct trust value $(T_{ij})_D$ is described in Fig. 5.

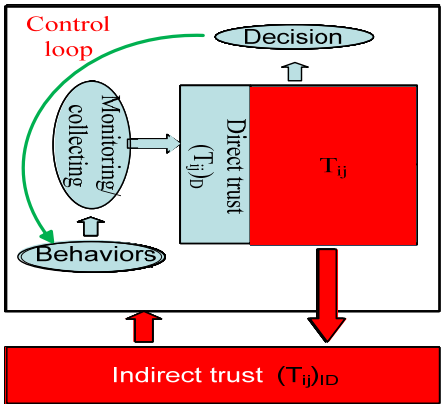


Fig. 4 The illustration of the proposed fault-aware and intrusion-aware scheme

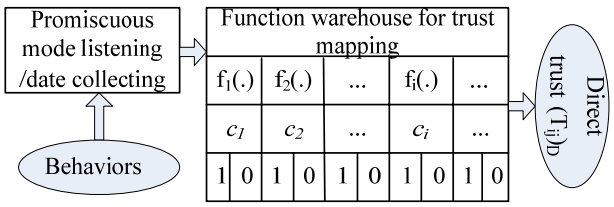


Fig. 5 The implementation of monitoring and computing for $(T_{ij})_D$

IV. Analysis of the Scheme's Performance of Fault-tolerance and Intrusion-tolerance

This paper introduces three kinds of misbehaviors in IP networks, e.g., self-faults, bad mouth attacks and conflict behavior attacks. We will discuss the performance of our scheme to tolerate the above misbehaviors.

A. How to Tolerate Self-Faults

The nodes in IP networks could be power off or malfunctions by some other artificial causes. Then this scheme will conclude that the direct trust value is "0" or very small according to Definition (2). The indirect trust value will decrease according to Definition (4). Above all, the final trust value of the node will decrease quickly. So the scheme can efficiently avoid this kind of faults.

B. How to Tolerate Bad mouth Attacks

If the node's recommendation is taken into consideration by other nodes, the malicious nodes can provide dishonest or false recommendations [3] to frame up good nodes and/or boost trust rating values of malicious nodes. This attack is named as bad mouth. Many existed contexts (e.g., [3] [7]) about trust management or reputation system have discussed this kind of attack.

Firstly, as mentioned above, comparing the indirect trust value with the average of the received indirect trust values, if the difference is less than the threshold, we will take the indirect trust value as fake information and ignore it. Secondly, if the difference is between the defined threshold and the threshold defined in Definition (4) we will use the weight of $\frac{1}{2^k}+\frac{1}{2^t}$ defined in Definition (4) to compute the trust value. It will take both the degree of the node and the time span below the threshold to weight. For one reason, as we all known, the bigger the degree of the malicious node is, the more harmful it is. So we could use the degree as the negative index of the weight. Then the weight decreases quickly with the growth of the degree. We insure not only the high efficiency but also the security. For another reason, the initial weight of the malicious node is "1". We customize a timer t equals to T_t (T_t>0). If the node recovers from the state of malicious we will set the weight to double but not beyond "1"and the timer t to "0". Otherwise, we will set the weight to half and the timer t to $2T_t$……. As described above, this scheme can effectively defense the bad mouth attacks.

C. How to Tolerate Conflict Behavior Attacks

Malicious node can impair good nodes' recommendation trust by performing differently to different nodes. For example, the node b behaves friendly to j and hostile to k. Then the opinions about node b are reverse between nodes j and k, leading conflict behavior. In our trust scheme, we can avoid this kind of attack by using of the weight strategy mentioned above.

V. Numeric Simulations and Performance Analysis

A. Simulation Scenarios

For simplicity, we just define and use two functions $f_1(.)$ and $f_2(.)$ for trust mapping. The function of $f_1(.)$ is defined as the packet delivery ratio and described below in Definition (5).

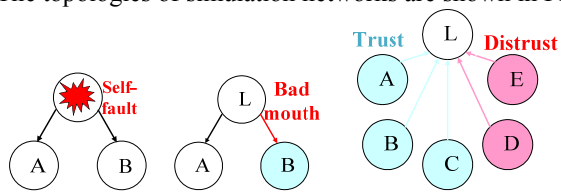
$$f_1(\cdot)=\frac{packet\_received\_number}{packet\_sent\_number} \tag{5}$$

$f_2(.)$ is the function of time delay described in Definition (6).

$$f_2(\cdot)=\mu\frac{packet\_delayed\_number}{packet\_sent\_number} \tag{6}$$

Here, parameter μ is related to the sensitivity of the time delay and can be adjusted by customers. For example, the audio and video services are sensitive to the time delay, and then μ will be bigger. The file transportation service is not sensitive to time delay then it will be smaller.

The topologies of simulation networks are shown in Fig. 6.



(a) For self-faults and bad mouth attacks (b) For conflict behavior attacks

Fig. 6 The topologies of the simulations

Here, Fig. 6(a) shows the conditions of self-faults and bad mouth misbehaviors in IP networks. Circumstance one: node L is power off. Circumstance two: node L is the attacker and behaves well to node A and badly to node B for ever. Fig. 6(b) shows the conflict behavior attacks. Node L is the attacker and behaves well to nodes A, B and C but badly to nodes D and E.

B. Simulation Results, Analysis and Estimation

In this paper, the trust values, which demonstrate that the nodes are good or bad, are updated in real time. It also can provide basis for the later use of separation and recovery strategies.

Case one in Fig. 6(a), the node L is broken down. Then, the trust value of node L in nodes A and B will both decrease quickly, which is shown in Fig. 7. So the nodes A and B will break off the friendship with node L.

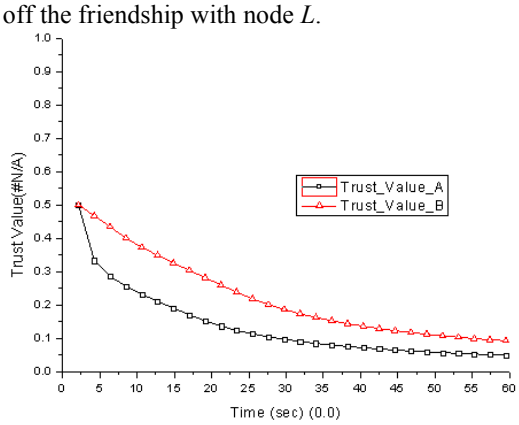


Fig. 7 Tolerance to self-fault

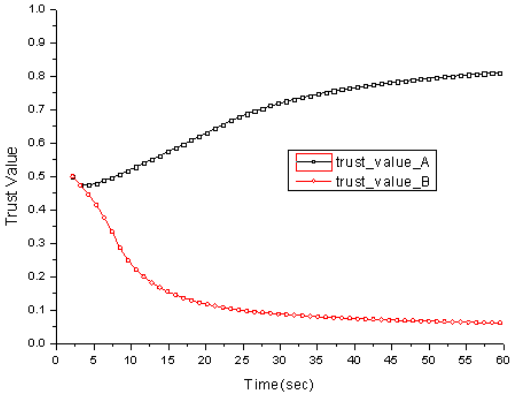


Fig. 8 Resiliency to bad mouth attacks

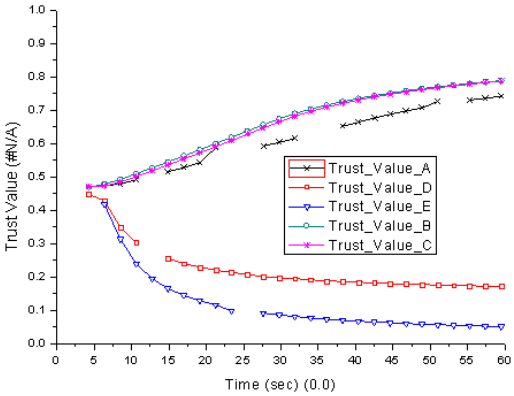


Fig. 9 Survivability to conflict behavior attacks

Case two in Fig. 6(a), the node *L* behaves well to node *A* and badly to node *B* for ever. Then, the node *L's* trust value in node *A* rises quickly and the trust value in node *B* decreases fast. So node *A* continuously contract with node *L*, while node *B* will not contract with node *L* with the drop of the trust value. According to Definition (1) the trust values of nodes *A* and *B* about node *L* is shown in Fig. 8.

The case in Fig. 6(b), according to Definition (1), the trust values of node *L* in nodes *A, B* and *C* will ascend quickly but descend in nodes *D* and *E*. The details are shown in Fig. 9. Therefore, nodes *A*, *B* and *C* can go well with node *L* but nodes *D* and *E* can not.

VI. Conclusions

In this paper, we design an efficient resilient scheme based on trust relationship for IP networks. Also, this scheme describes the relationships between the trust rating and the network behavior qualitatively .When a node's behavior threaten other nodes, its trust rating in these nodes will be decreased. Moreover, we give the propagation of the trust rating in IP networks and analyze the scheme how to tolerate three kinds of known malicious behaviors, i.e., self-faults, bad-mouth attacks and conflict behavior attacks. Last but not least, this scheme can detect the misbehavior nodes exactly and make contribution to the separating and recovering strategies which will be developed in our future works.

Acknowledgments

Supported by National Key Basic Research Program (973 Program: 2007CB310706), National Science Fund for Distinguished Young Scholars (NSFDYS: 60725102), Research Fund for the Doctoral Program of Higher Education (RFDP: 20060614018), National High Technology Research and Development Program of China (863 Program: 2007AA01Z246, 2007AA01Z227), National Nature Science Foundation of China (NSFC: 60672045).

References

[1] P. Resnick and R. Zeckhauser, "Trust among strangers in internet transactions: Empirical analysis of ebay's reputation system." *Advances in Applied Microeconomics: the Economics of the Internet and E-Commerce*, vol.11, pages 127-157, November 2002.

[2] S. Buchegger and J.-Y. Le Boudec. "Performance analysis of the CONFIDANT protocol (Cooperation of Nodes-Fairness in Dynamic Ad-hoc Networks)," *in Proceedings of MobiHoc* 2002, Lausanne, CH, June 2002.

[3] S. Ganeriwal and M. Srivastava. **"**Reputation-based framework for high integrity sensor networks," *in Proceedings of the 2nd ACM workshop on security of ad-hoc sensor networks (SASN'04),* October 25, 2004, Washington, D.C., USA.

[4] A. Srinivasan, J. Teitelbaum and J. Wu. DRBTS, "Distributed reputation based beacon trust system," *in the 2nd IEEE International Symposium on Dependable, Autonomic and Secure Computing (DASC'06),* Indianapolis, USA, 2006.

[5] Haiguang Chen, Huafeng Wu, Xi Zhou, Chuanshan Gao. **"**Agent-based trust model in wireless sensor networks," *in DOI 10.1109/SNPD.* 2007.122. 119~124

[6] Newman M E J. "The structure and function of complex networks," *in SIAM Review,* 2003,45:167~256

[7] C. Dellarocas, "Mechanisms for coping with unfair ratings and discriminatory behavior in online reputation reporting systems," *in Proceedings of ICIS*, 2000.

[8] Adil Abraham Kodian. Department of Electrical and Computer Engineering, University of Alberta. Advances in *p*-Cycle Network Design. *A thesis submitted to the Faculty of Graduate Studies and Research in partial fulfillment of the requirements for the degree of Doctor of Philosophy*. Spring 2006.

[9] Gangxiang Shen. Department of Electrical and Computer Engineering, University of Alberta. Design and Performance of Protected Working Capacity Envelopes Based on p-Cycles An Alternative Framework for Dynamic Survivable Network Service Provisioning. *A thesis submitted to the Faculty of Graduate Studies and Research in partial fulfillment of the requirements for the degree of Doctor of Philosophy*. Spring 2006.

[10] Piotr Cholda, Andrzej Jajszczyk. Reliability Assessment of Optical *p*-Cycles. *IEEE/ACM TRANSACTIONS ON NETWORKING*, VOL. 15, NO. 6, DECEMBER 2007.

[11] Haiguang Chen, Peng Han, Bo Yu, and Chuanshan Gao "A New Kind of Session Keys Based on Message Scheme for Sensor Networks". *The Seventeenth Asia Pacific Microwave Conference (APMC 2005)* Suzhou, China, Dec. 4-7, 2005.

[12] C. Karlof, N. Sastry, and D. Wagner, TinySec: A Link Layer Security Architecture for Wireless Sensor Networks, *Proceedings of the Second ACM Conference on Embedded Networked Sensor Systems (SenSys 2004)*, pages 162-175, November 2004.

[13] Haiguang Chen, Peng Han, Xi Zhou, Chuanshan Gao. Lightweight Anomaly Intrusion Detection in Wireless Sensor Networks. *PAISI 2007* LNCS 4430, pp.106-116.