International Journal of Advances in Computer Networks and Its Security
Volume 6 : Issue 1 [ISSN 2250-3757]
Publication Date : 18 April, 2016

Cellular Cross-layer Intrusion Detection and Response

Mohammad Raihan Kabir, Rifat Rahman and Md. Motaharul Islam

***Abstract*—Usage of data through cellular devices are growing exponentially due to the growing popularity of smart phones and tablets. Because of their smaller sizes and reduced capabilities, it is sometimes hard to impose adequate security measures to these everyday used devices. Thus they become a popular target for data theft and misuse. Because of the nature of cellular network various kinds of attack on the cellular devices such as distributed denial-of-service (DDoS) are happening frequently. Conventional security measures for the layered architecture cannot cope with this ever evolving security issue. Thus we have proposed an enhancement of cross-layer design for security in wireless network entitled as Cellular Cross-layer Intrusion Detection and Response (CXIDR). We have utilized the cross-layer design which integrates features from various layers for detecting intrusions in wireless environment and our proposed system enhances performance up to 20%.**

***Keywords*—cross-layer architecture, wireless network, cellular network, intrusion detection system, intrusion response system**

I. Introduction

Cellular network is a special type of wireless network distributed over large areas called cells, through the use of radio towers which are commonly known as base stations. These base stations work as a transceiver. In the network, each cell uses different frequencies from their neighbors, to avoid interference and provide bandwidth for necessary data transmission and through the use of smart phones and tablets a large amount of data is being transmitted every day where wireless technology is used as a backbone. A wireless network is any type of computer network that uses wireless data connections for connecting network nodes. Wireless networks are generally implemented and monitored using radio communication. Though wireless network has more advantage compared to wired network but still security of wireless network is a great issue. Some reasons of wireless network's being unsecured are mentioned in [1] and [5]. However, there are a great number of security risks associated with the current wireless protocols. Different kinds of security attacks are mentioned and discussed in details in [1] and [2]. Some of the renowned attacks are DoS attack, Sybil attack, Wormhole attack etc. Security solutions may be authentication, cryptography or key management. Security solutions are available recently nevertheless, they alone cannot prevent different kind of wide range of attacks. Normally, security measures are provided in the application layer. Layered approach is fit for wired network but not for wireless network. In [3] the solution of this is discussed. The researchers are now interested in cross-layer design techniques to alleviate the problems of layered architecture. Some reasons of choosing cross-layer design are mentioned in [5].

Cross-layer design which is unlike the layered architecture refers to designing of interfaces, protocols or architectures. It utilizes inter-layer interactions that is a superset of the standard interfaces for achieving better performances and facilitating new features. One of the most important features of cross-layer design is sharing information between two or more layers. The idea behind cross layer information exchange is to use various parameters from different layers for joint optimization of protocols across the communication stack. In [3] different cross-layer design approaches are discussed briefly. Cross-layer architecture and its security as an emerging concept have many opportunities. There are many proposals regarding this topic. Physical layer data can be passed to application layer and reverse is also possible. Besides, adjacent two or three layers can be merged together that is called a super-layer. Research scope regarding security in cross-layer is increasing recently and many works have been done. But yet, implementation is not that much satisfactory.

Intrusion detection system (IDS) is an important security aspect in wireless network. It detects the misbehaving and malicious nodes and isolates them. Researchers have recently proposed some IDS approaches which is discussed in [1]. From [1] and [4] it is noticed that IDS can classify attacks by misuse, anomaly or specification-based system. Besides of existing approaches, different kinds of new cross-layered approaches are discussed in [5] and [6] including cross-layer design for intrusion detection. Most of the attackers are now trying to attack wireless networks as they are easy to hack and misuse. So, security measures need to be taken to prevent attacks in wireless networking are quite challenging.

In this paper, we have proposed a new IDS system that combines both wireless network and cross layer framework which is better than its counterparts in many aspects. In case of false positive and false negative reduction purpose, our system works 3%-5% and 5%-8% better than its counterparts respectively. It has been observe that comparing between CXIDR, XIDR and single layer, our

Mohammad Raihan Kabir
Islamic University of Technology
Bangladesh

Rifat Rahman
Islamic University of Technology
Bangladesh

Md. Motaharul Islam
Islamic University of Technology
Bangladesh

system performs the best among the three. We have also introduced various packet management techniques to supply our detection information with least amount of time. We have also proposed two databases which will store all the information about the attacks and our responses in respect to them. Just by detecting we cannot solve our problem. We have to response to the threats. So we have also proposed a response module engine which will select a cost-effective response.

II. Related works

'Cross Layer Design' has become a new buzz word in wireless technology. Through experience the researchers have learned that there are many problems regarding wireless network which do not occur in wired networks. To cope up with these new kinds of problems collaboration between various OSI layers have been proposed.

In [3] Vineet Srivastava et al. have tried to give us a rough picture of cross layer architecture and various proposals given by researchers regarding this. The authors have given us a clear idea about how cross layer design can be implemented such as: creating new interface between layers, creating super-layers, designing coupling without creating new interfaces or by vertical collaboration. They also have described how different layers can pass information among each other. They proposed three methods like direct communication (through data packets), shared database or by creating new abstractions.

In [4] Jatinder Singh et al. proposed a new method to detect intrusion with the help of cross layer design. In the proposed mechanism, the Received Signal Strength (RSS) and the TT value (the time it takes for RTS-CTS handshaking) are the identifying merit here. A dynamic profile is created based on these measures. As no two devices can have the same values it is a very good identifier. If a node has higher RSS value than the threshold, then that device is identified as an attacker. The threshold values are updated periodically and are managed in the base stations.

Igors Svecs et al. presented a complete intrusion detection and response framework named Cross-layer Intrusion Detection and Response (XIDR) in [6]. According to them this framework utilizes multi-source IDS and cross-layer automated intrusion response system to deploy cost-effective and efficient pre-emptive responses. It is used to detect intrusions in wired environment. They have provided a model which includes multiple intrusion detection sources, data sources, automated response selection engine and a collection of response deployment modules. They have also improved the response engine and provided a diagram of XIDR deployed in test-bed environment. Their proposed framework was Host Intrusion Detection System (HIDS) that runs on individual hosts in the network and it monitors the incoming and outgoing packets from the hosts and will alert the user or administrator when suspicious behavior is detected. Finally, the authors have shown some simulation results which show the efficiency of cross-layer approach over the single layer approach in detecting intrusions.

III. Major Challenges

In our endeavor to develop a new IDS system we have faced various fundamental challenges. Some of them we have overcome, some of them we still are trying to get our head around. The major challenges are briefly explained below:

A. *Wireless nature of communication:*

As the network architecture is wireless, packets may come from anywhere in a broadcast fashion. That means anyone can pick up the packet and modify, change or simply fabricate it. .

B. *IP Address spoofing*

IP addresses are dynamically allocated to mobile devices but it sometimes let the attacker impersonate as a legitimate user.

C. *Implementing IDS in cross layer design:*

In wireless architecture, implementing IDS itself is a challenge. To use cross layer design is probably one of the newest research points in this sector which is difficult too.

D. *Creating NIDS*

All the research about a wireless IDS system has been host based. In this respect, NIDS system has been relatively untouched. So, we have to carefully consider various aspects of the network and the system's feasibility against HIDS

IV. Our Proposed Framework

We are proposing a new cross layer IDS system which will effectively perform its task against any kind of intrusion. Our proposed architecture has 4 modules. These are as follows:

A. Intrusion Detection Module (IDM).
B. Detection Database.
C. Dynamic Response Selection Module (DRSM).
D. Response Deployment module (RDM).

In Fig. 1, detail architecture of our proposed system has been shown:

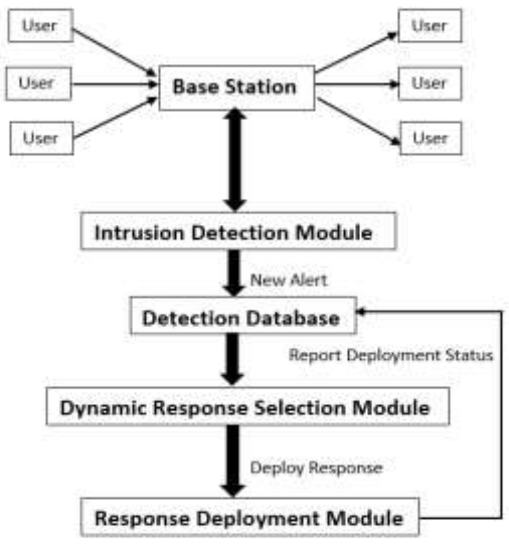


Figure 1. CXIDR Framework.

A. *Intrusion Detection Module (IDM):*

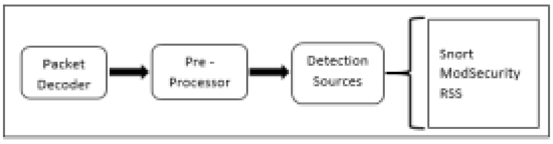


Figure 2. Intrusion Detection Module

Our Intrusion Detection Module combines various techniques and implements cross layer architecture for detection method. In Fig. 2 IDM has been shown in detail.

1. Packet Decoder

Our system's detection techniques sometimes need the packet to be accessed in different layers. But in a base station all packet is relayed to its destination. So it doesn't need to decode the packets. So we introduce our own packet decoder. With this we will decode our packet to detailed analysis through various techniques such as Snort, RSS or ModSecurity. These methods also need the headers attached by various layers of open system interconnection (OSI) model.

2. Pre-processor

After decoding now we have the headers of several layers of OSI models like physical, network, transport, application layer etc. As our techniques use different layer headers and the data it encapsulates, we supply those modules with the proper headers and data segment. In this way we can save time which would have been wasted if they had to sort.

3. Detection Sources

We use various detection techniques. They give us the ability to analyze a packet in a cross layer environment. These techniques are briefly discussed below:

a. *Snort*

Snort is an open source intrusion detection system. It combines the benefits of signature, protocol, and anomaly-based inspection. It is the most widely deployed IDS/IPS technology in modern world.

b. *ModSecurity*

Array of request filtering and other security features is supplied by ModSecurity to the Apache HTTP Server, IIS and NGINX. ModSecurity is a web application layer firewall. It is an open source software.

c. *RSS*

RSS means Received Signal Strength. This value is unique to the sender and receiver. When a call is initiated the signal strength from the sender and receiver is recorded and the time it takes to reach them is also recorded. When the packets pass through the base station then the RSS value is checked. If the RSS value is greater, we understand that there is an intruder in the network and take necessary action. After the incoming packet has gone through all the sources, if an intrusion is detected then the necessary information is passed to Dynamic Response Selection Module through Detection Database and then an appropriate response is generated. A detail of RSS is described in [4].

B. *Detection Database*

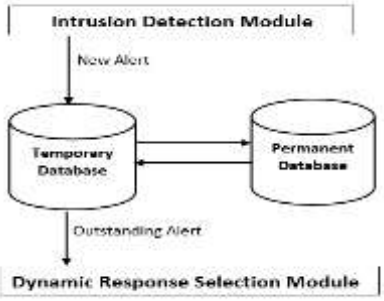


Figure 3. Detection Database.

Detection Database stores all the information of our intrusions detected so far and all the intrusion that we have detected in the life time. There are two kinds of database:-

1. Temporary Database:

This database stores all the information about the recent attacks like attack type, layers associated, threat level, generation source and all the info about the source generation it. After a certain amount of time the information is saved into the permanent database.

2. Permanent Database:

This database stores all attacks the system has faced so far and the responses to them. It stores a detailed description from the attack occurring to the time where the system has deemed the attack to be nullified. It stores the information on which responses were used and how much cost effective it was. It is a permanent sink for all the information and the system's effectiveness in it for future consultation.

C. *Dynamic Response Selection Module (DRSM):*

After receiving all the necessary information about the current attack and if there was a similar past attack from the same or different source a cost effective response is generated. To do so we need two things. They are:

1. Response Selection Engine
2. Response Rules Database

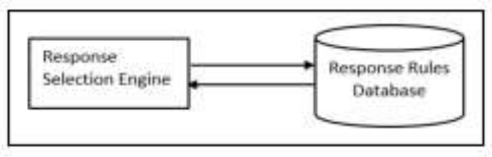


Figure 4. Dynamic Response Selection Module.

1. *Response Selection Engine:*

This engine executes the selection algorithm for choosing a cost-effective response. At first it receives information like threat level, layers associated with the attack, the detection source and all the associated information as well as what the system did in case of an attack of similar caliber from the detection database. Then a query is executed to fetch the response appropriate with the threat level and the layers associated with the attack. There can be various responses regarding a single kind of attack. Such as DOS attack and DDOS attack. In sense they are the same. But they might attack different layers thus having different rules. These rules are classified in case of cost which is associated with the threat level. If the threat is high, we may employ solution with greater cost and vice versa. The engine fetches all the responses and on the value of cost and threat level chooses a cost-effective response which is passed to Response Deployment Module.

Response Selection Algorithm:

```
Input:
(ID, DATETIME, SOURCE_IP, DESTINATION_IP,   DESCRIPTION,
TYPE, SOURCE_MODULE, DEPLOYMENT_MODULE, PRIORITY,
RELATED_LAYERS, RESPONSE).CXIDR_TEMPORARY_DATABASE

(RESPONSE_ID, DESCRIPTION, SOURCE_MODULE,
DEPLOYMENT_MODULE, TYPE, RELATED_LAYERS, PRIORITY,
COST, RESPONSE).CXIDR_
RESPONSE_RULES
Output: RESPONSE
Steps:
1.    Select all RESPONSE where

PRIORITY.CXIDR_ TEMPORARY_DATABASE ==
PRIORITY.CXIDR_RESPONSE_RULES          && RELATED_LAYERS.
CXIDR_TEMPORARY_DATABASE == RELATED_
LAYERS.CXIDR_RESPONSE_RULES

2.    If (Count(RESPONSE)>1) {
          Select RESPONSE with Min (COST) ;}
3.    Else If (Count(RESPONSE)==1) {
          Select RESPONSE ;}
4.    Else {
          Select DEFAULT RESPONSE ;}
```

In summary, using the response selection algorithm we select the response by matching the priority and OSI layer from the two tables *CXIDR_TEMPORARY_DATABASE* and *CXIDR_RESPONSE_RULES*. If multiple responses are found, our response selection engine will select the response from the *CXIDR_RESPONSE_RULES* with the lowest cost. If there is only a single response is found, that response will be selected by the selection engine. But if there is mismatch in the two tables, no response will be selected and a default response will be generated.

2. *Response Rules Database:*

This database stores all the responses and it can be easily updated. Whenever the Response Selection Engine needs a response, they are generated from here

D. *Response Deployment Module (RDM):*

This module deploys the responses selected by DRSM. At first, the response is received from the DRSM and it follows necessary protocol to carry out the response. It also will calculate success rate and then send that information to Detection Database for future storage and consultation. Our framework will use physical, transport and application layer. Through the use of RSS value, we have used physical layer values of RSS and supplied them to the application layer. ModSecurity and Snort are used in application layer.

V. Performance Evaluation

We have used Network Simulator-3 or NS-3 to simulate RSS. We have also compared our system's performance with Single Layer and XIDR. In Fig. 5 and Fig. 6 false positive and false negative reduction is shown.

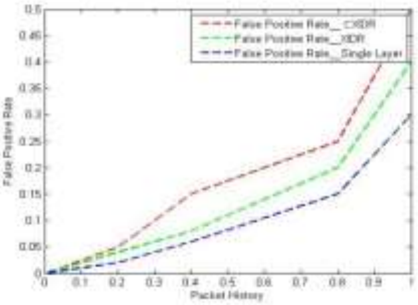


Figure 5 False Positive Reduction.

In both figure, packet rate is in X-axis. In Fig. 5 false positive rate and in Fig. 6 false negative rate is in Y-axis. So, from both this figure it has been shown that our system performs better than others.

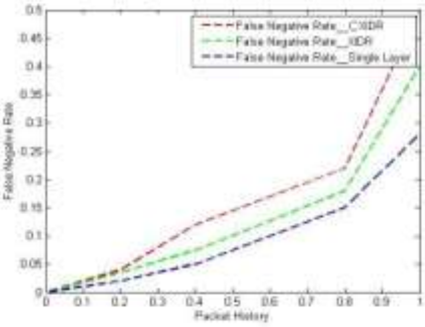


Figure 6. False Negative Reduction.

In Table 1 and Table 2 there are two table of comparisons showing the false positive and false negative comparison respectively among Single Layer, XIDR and CXIDR. This comparison is done with respect to random packet rate. These data is used to draw the graphs of Fig.5 and 6. The graphs are drawn with the help of MATLAB. We have collected data manually from Snort, RSS and ModSecurity.

TABLE 1. FALSE POSITIVE REDUCTION COMPARISON

Packet History	Single Layer	XIDR	CXIDR
0	0	0	0
2	0.5	0.4	0.2
4	1.5	0.8	0.6
8	2.5	2	1.5
10	5	4	3

TABLE 2. FALSE NEGATIVE REDUCTION COMPARISON

Packet History	Single Layer	XIDR	CXIDR
0	0	0	0
2	0.4	0.35	0.2
4	1.2	0.75	0.5
8	2.2	1.8	1.5
10	5	4	2.8

In Fig. 7 intrusion detection comparison among single layer, XIDR and CXIDR is shown and intrusion detection rate is in Y-axis. From this figure it is shown that CXIDR has more success in detecting intrusions than other systems.

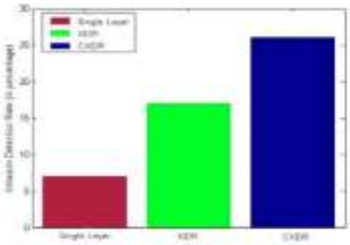


Figure 7. Intrusion Detection Comparison.

We have used Oracle Database 10g Express Edition to create various tables which is used in our algorithm. To implement our algorithm, we connected the Oracle with Java using NetBeans IDE 7.1.2. For our implementation purpose we have created two tables in Oracle which are shown in Table 3 and Table 4.

TABLE 3. CXIDR_TEMPORARY_DATABASE

ID	DATETIME	SOURCE_IP	DESTINATION_IP	DESCRIPTION	TYPE	SOURCE_MODULE	DEPLOY_MODULE
01A	10/07/2014	10.22.5.31	10.22.6.36	XXX	YYY	SNORT	DDD
02A	13/7/2014	10.22.5.35	10.22.6.56	FGF	GGF	RSS	TTD
031	22/7/2014	10.22.5.31	10.22.6.36	PPP	HHH	RSS	GGG

TABLE 4. CXIDR_RESPONSE_RULES

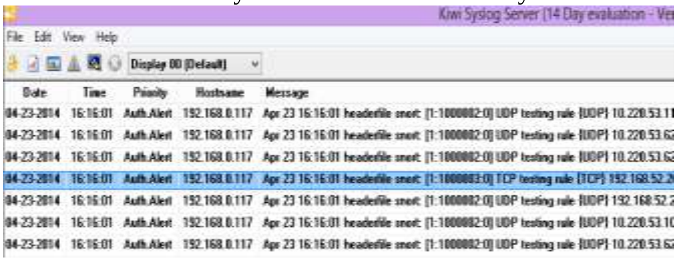
RESPONSE_ID	DESCRIPTION	TYPE	SOURCE_MODULE	DEPLOY_MODULE	PRIORITY	RELATED_LAYERS	COST	RESPONSE
20X	XXX	YYY	SNORT	DDD	3	Application	2	ABORT
21X	FGF	GGF	RSS	TTD	3	Application	4	DO_SOMETHING
22X	GHT	XXCX	RSS	GGG	2	Network	4	Caution

Information of CXIDR_TEMPORARY_DATABASE table and CXIDR_RESPONSE_RULES table are shown in details in Table 3 and Table 4. The response selection algorithm is coded in Java language using NetBeans software. Here, ojdbc6 JAR library is used for this implementation process. The output of the sql query of our implemented algorithm is displayed in Table 5. Using this response some conditions will be applied upon them with respect to cost according to the response selection algorithm and response with the minimum cost will be deployed by the Response Deployment Module.

TABLE 5. RESULT OF SQL QUERY

PRIORITY	RESPONSE
3	ABORT
2	CAUTION
3	DO_SOMETHING

In Fig. 8 application of Snort is shown. We have implemented Snort with the help of Kiwi Syslog Server which is used as a Graphical User Interface (GUI) for showing the analysis of incoming and outgoing packets. From this sort of analysis intrusions can be easily detected.



```
Date        Time      Priority    Hostname        Message
04-23-2014  16:16:01  Auth.Alert  192.168.0.117   Apr 23 16:16:01 headerfile snort: [1:1000002:0] UDP testing rule {UDP} 10.220.53.11
04-23-2014  16:16:01  Auth.Alert  192.168.0.117   Apr 23 16:16:01 headerfile snort: [1:1000002:0] UDP testing rule {UDP} 10.220.53.62
04-23-2014  16:16:01  Auth.Alert  192.168.0.117   Apr 23 16:16:01 headerfile snort: [1:1000002:0] UDP testing rule {UDP} 10.220.53.62
04-23-2014  16:16:01  Auth.Alert  192.168.0.117   Apr 23 16:16:01 headerfile snort: [1:1000003:0] TCP testing rule {TCP} 192.168.52.2
04-23-2014  16:16:01  Auth.Alert  192.168.0.117   Apr 23 16:16:01 headerfile snort: [1:1000002:0] UDP testing rule {UDP} 192.168.52.2
04-23-2014  16:16:01  Auth.Alert  192.168.0.117   Apr 23 16:16:01 headerfile snort: [1:1000002:0] UDP testing rule {UDP} 10.220.53.10
04-23-2014  16:16:01  Auth.Alert  192.168.0.117   Apr 23 16:16:01 headerfile snort: [1:1000002:0] UDP testing rule {UDP} 10.220.53.62
```

Figure 8. Packet Analysis Using Snort.

Implementation of Received Signal Strength (RSS) is done using NS-3. Here, Signal to Noise Ratio or SNR is counted. We have used this value as RSS in our system. The SNR value is calculated and then converted into SNR db (Decibel). In Table 6, the packet rate and RSS value in decibel is displayed.

TABLE 6. PACKET RATE AND CORRESPONDING RSS VALUE

Packet	RSS(Decibel)
1	119.35
5	123.077
7	257.859
10	257.859
100	257.859

VI. Conclusion

In this paper, we have introduced a novel IDS framework that combined multiple intrusion detection sources and utilized it in cellular environment. We have also introduced a cost-effective response selection module across various layers. We showed that our proposed CXIDR methodology is capable to outperform the conventional one. In future, we shall enhance CXIDR further and add some other security related features with the current system. There may be some other works of implementing the algorithm and building a response deployment module so that present CXIDR can face the upcoming challenges in the future. The methodologies we proposed in this article are based on new technologies and it might be a complete scheme to safeguard our precious data and devices.

References

[1] A. Abduvaliyev, A. S. K. Pathan, J. Zhou, R. Roman and W. Wong, “On The Vital Areas of Intrusion Detection Systems in Wireless Sensor Networks”, IEEE Communication Surveys & Tutorials, vol. 15, no. 3, Thirdquarter 2013.

[2] A. S. K. Pathan, H. W. Lee and C. S. Hong, “Security in Wireless Sensor Networks: Issues and Challenges”, International Conference on Advanced Communications Technology, pp. 1043-1047, Feb. 20-22, 2006.

[3] V. Srivastava, M. Motani, “Cross-Layer Design: A Survey and the Road Ahead”, IEEE Communications Magazine, pp. 112-118, Dec. 2005.

[4] J. Singh, L. Kaur and S. Gupta, "A Cross-Layer Based Intrusion Detection Technique for Wireless Networks", The International Arab Journal of Information Technology, Vol. 9, No. 3, pp. 201-206, May 2012.

[5] M. Xiao, X. Wang and G. Yang, "Cross-Layer Design for the Security of Wireless Sensor Networks", Proceedings of the 6th World Congress on Intelligent Control and Automation, pp. 104-108, June 21 - 23, 2006, Dalian, China.

[6] I. Svecs, T. Sarkar, S. Basu and J. S. Wong, "XIDR: A Dynamic Framework Utilizing Cross-Layer Intrusion Detection for Effective Response Deployment", 34th Annual IEEE Computer Software and Applications Conference Workshops, pp. 287-292, 2010.

[7] H.T.T. Nguyen, M. Guizani "An Efficient Signal-Range-Based Probabilistic Key Predistribution Scheme in a Wireless Sensor Network", IEEE Transactions On Vehicular Technology, Vol. 58, No. 5, pp. 2482-2487, June 2009.

[8] S. Shakkottai, T. S. Rappaport, P. C. Karlsson, "Cross-layer Design for Wireless Networks", June23,2003.

[9] P. Liu, Z. Tao, Z. Lin, E. Erkip, S. Panwar, "Cooperative Wireless Communications: A Cross-layer Approach", IEEE Wireless Communications, pp. 84-89, Aug. 2006

[10] S. Shakkottai, T. S. Rappaport, P. C. Karlsson, "Secure Routing Protocol Using Cross-Layer Designed Energy Harvesting in Wireless Sensor Networks", June23,2003.