Journal of Computer Science 10 (12): 2366-2373, 2014
ISSN: 1549-3636

doi:10.3844/jcssp.2014.2366.2373 Published Online 10 (12) 2014 (http://www.thescipub.com/jcs.toc)

WIRELESS MESH NETWORK CROSS-LAYER INTRUSION DETECTION

[1]F.S. Al-Anzi and [2]S. Khan

[1]Computer Engineering Department, Kuwait University, Kuwait
[2]Kohat University of Science and Technology (KUST), Pakistan

Received 2014-04-29; Revised 2014-06-10; Accepted 2014-11-26

ABSTRACT

Intrusion is something which is unsolicited activity and which might be used to interrupt the functions of wireless network. If we talk about wireless networks, having centralized monitoring policy; therefore it is very much easy to detect and eliminate intrusions efficiently. But when we look forward to wireless scenario, especially in the multi hop wireless network, intrusion activities are more because of the lack of centralized monitoring policy. Wireless network is very much vulnerable to different kinds of attacks and intrusions at different OSI layer due to mainly co-operation among their noses. Intrusion detection is the most fundamental component of defense in depth strategy, are capable to identify security attacks and raise an alarm to inform authorities. Intrusion detection system, a passive defense strategy informs about attacks to network administrator because the attacks come easy to wireless network. Intrusion detection system is a second line of defense. Lots of IDSs are proposed in the literature, capable to detect attacks in a particular layer of the OSI model. Here we are proposing Cross layer IDSs, which is capable to detect multiple layer possible attacks.

Keywords: Wireless Mesh Network, Security, Intrusion Detection System, Cross Layer

1. INTRODUCTION

Wireless Mesh Network (WMN) has primarily two types of architectures such as infrastructure-based and infrastructure-less WMN (Khan *et al*., 2008a). Infrastructure-based network has mesh clients, mesh routers and fixed and wired Mesh gateway. “Base station” is known as bridge of the network. Infrastructure-based network is no doubt very desirable service to provide ubiquitous broadband service for a wide range of geographical area. Mesh routers form the infrastructure for clients in Multi hop fashion and it is very easy to implement and extend. Mesh router can be connected to internet by gateways and form a mesh of self-healing link among themselves. Infrastructure-based WMS supports both static and mobile nodes.

Infrastructure-less WMN is a kind of peer-to-peer or ad hoc networks among client device in which there is no support of Mesh router or gateway. Infrastructure-less network router is not necessary because nodes have routing capability between sources to destination. In this case highest level communication occurs. It is extremely necessary to design such mechanism for WMNs which use fewer resources and light weight. The reason is that infrastructure-less WMNs have many design constraints such as low energy, low bandwidth, limited processing, memory constraints and are highly vulnerable to many security attach such as passive, active and Denial of Service (DoS) (Khan *et al*., 2008b). There are lots of security issues present in the multi hoop decentralized network such as WMN. A network is said to be secure, if it ensure all time availability, data integrity and provides privacy for both user and data

Corresponding Author: F.S. Al-Anzi, Computer Engineering Department, Kuwait University, Kuwait

in transit (Djenouri *et al*., 2005). Many solutions of WMN security have been proposed, however, those solutions are either for few security attacks (Khalid and Mahboob; Meghanathan, 2013). Similarly, majority of the solutions so far are proposed to secure network layer of WMN (Khan *et al*., 2010a; Shah *et al*., 2013). Security mechanisms of network layer are only to tackle few attacks, but they are not fully able to take care the entire physical layer and MAC layer attacks. There is a security mechanism known as Light weight intrusion detection system for WMN, are powerful, small and flexible to be used as permanent elements of network security. Lightweight IDS can be easily configured and deployed in any node of the network. The nature of IDS is passive and does not provide primary defense against security attacks. Many classes of IDSs are designed, in which rule based uses attack signature in a database to detect intrusions, while anomaly based uses network patterns and any deviation in pattern, consider as an attack (Northcutt and Novak, 2002; Khan *et al*., 2010b). Intrusion and attacks are detected by IDS at a particular layer but cannot detect other layer so we use cross layer methodology, capable to identify the different layers of attack and intrusions and raise an alarm. The concept of cross layer methodology says that for decision making different parameters of different layers should be considered. We analyze different cross layer IDSs designed for WMNs. In our research paper, we propose cross layer based framework of IDS for WMN. The proposed IDS is tested in different scenarios. Regardless of its limitations, the proposed mechanism is can be highly efficient in detecting various security attacks.

The paper is organized as follows. Section 2 analyzes different IDS. Section 3 presents proposed IDS. Results are described in section 4. Section 5 consists of a conclusion.

2. RELATED WORK

Network security is a prominent requirement of multi hop wireless network and IDS is the more classical approach of network security. Intrusion detection system is a passive defense, trying to differentiate abnormal activities from normal one. IDS monitor events occurring in networks and alarm depending on how they evaluate the network traffic. Different types of IDS are available in the literature such as anomaly IDS, network or host based IDS and Passive IDS. Most of the IDSs are designed to operate on the network layer and detect only network layer anomaly. Since multi hop wireless network is vulnerable to security attack at various layers, i.e., physical layer, data link layer, network layer, transport layer and application layer. So cross layer IDSs have a unique feature to monitor different cross layer attacks. In literature, many IDSs are proposed (Chen *et al*., 2007). Some security mechanism are protocols based such as Watchdog and pathraters (Rafsanjani *et al*., 2008; Caballero, 2006). Watchdog method (Rafsanjani *et al*., 2008) allows detecting misbehavior node. These are used to select secure path and are capable to detect network layer attach by listening all the nodes in promiscuous mode. In a sure path every node should forward the traffic if any node does not, then it is tagged as misbehaved. CONFIDANT (Rocke and Demara, 2006) is another secure mechanism which is used to observe neighbor activity and observe misbehavior. CONFIDANT is an improved version and solve Watchdog and pathrates problem. A misbehaving node cannot be used in routing and cannot send packets. TARA (Shrobe *et al*., 2007) is a path secure architecture which encrypts the packets and also report about broken paths. Cross layer design consists of feedback system and provide information via layer boundary. Unlike OSI model, cross layer design removes strict boundaries between layers and allow communications. Cross layer design is a relatively new security technique which provides a common platform for different layers to exchange parameters so that to detect multi-layer security attack (Khan *et al*., 2009). IDS systems proposed by (Da Silva *et al*., 2005; Onat and Miri, 2005) contain Consist of nodes known as “monitor mode” in the network, which are responsible for monitoring their neighbors, looking for intruders. Wang *et al*. (2009) describes crossed layer based anomaly detecting in WMN (Wang *et al*., 2009) and develop a prototype using the concept of cross layer information exchange between the data link layer and the network layer. Boubiche and Bilami (2012) proposed a cross layer intrusion detection agent for distributed networks (Boubiche and Bilami, 2012). In this scheme parameter is collected from different layer by data module. Khan *et al*. (2010b) proposed a real time cross layer detection mechanism for WMNs (Khan and Loo, 2009). The network layer and MAC layer parameters are exchanged in this mechanism for detection of different kinds of attack. This method explains the severity of attack by maintaining three different profiles. The detection rate of this scheme is high, but can only detect flooding attacks. Thamilarasu *et al*. (2005) proposed a cross layer IDS for distributed ad-hoc network (Thamilarasu *et al*. 2005). The proposed scheme have two level of intrusion detection, level 1 and 2, information of data link layer is exchanged with network layer to detect malicious activity. This scheme is good for packet misdirection and packet drop attack.

Liu *et al*. (2006) proposed a cross layer based IDS with a combination of data mining technique. A specific feature sets are defined to locate the attacks within one hop range (Liu *et al*., 2006). Here we propose a novel cross layer intrusion detection system where MAC layer and network layer parameters are exchanged and provide a wide range of protection against many security attacks.

Paper is one part of the entire proceedings, not an independent document. Please do not revise any of the current designations.

3. PROPOSED CROSS LAYER IDS

The proposed IDS has a capability to detect multiple layers of attacks by using the concept of cross layer methodology in which parameters are exchanged in different layers.

3.1. Assumptions

Here we take infrastructure less network and assume WMN consist of both static and mobile nodes. Infrastructure network has no support of routers and gateways. All the nodes in the network have routing capability to communicate with its neighbors and form multi hop communication model.

3.2 Design Considerations

Since infrastructure less WMN has many limitations in terms of energy, data rate, memory, processing and mobility. Ideal IDS for WMNs should be:

- Lightweight in nature to preserve the limited resource
- The capability to detect multi-layer security attack

3.3. Framework

Our proposed IDS work at each node, as soon as an attack is detected, information of malicious activity is passed to another neighbor node in communication range. The proposed IDS consist of 5 modules: Data collection module, analysis module, detection module, classification and alarm module. The framework is presented in **Fig. 1**.

3.3.1. Interaction Interface

The interface is a contact point between layers and applications. The main objective of the interface is to manage all sub interfaces and provide access to lawyers.

3.3.2 Cross Layer Data Module

Cross layer data module houses data in a very unique way so that every layer protocol access it efficiently. It also maintains up to date data for the cross layer interface. Cross layer data collection module collects:

- Signal strength and battery power from physical layer
- Mobility, data rate, link parameters and throughput information from MAC layer
- Packets sent, packets received, TTL, frequency of route failure information from the network layer
- Congestion and transmission control information from transport layer

All the collected parameters are forwarded to the analysis module to analyze any anomaly and this IDS maintains normal behavior of each and every parameters. Any difference in normal behavior is seen and information fetch to detection and classification module. The most important part of our framework is attack module which detects type of attack by signature of various attacks. When an attack is detected another module raises an alarm **Table 1**.

3.3.3. Proposed Algorithm

Proposed IDS houses some new features with having a traditional layer architecture. The basic idea of IDS is to detect multilayer intrusions and attacks. At the physical layer every node knows the signal strength send by its neighbor node, so any anomaly is detected in the physical layer by comparing the difference in signal strength. Our proposed IDS takes different parameters from different layers and detect any undesirable behavior of the node and raise an alarm.

Table 1. Threats in WMN and different parameters

Layer	Threat	Parameters
Physical layer	Scrambling, jamming	Channel switching frequency, battery power, signal strength
MAC layer	Dos attack, rouge mesh node attack, identity theft, Eave-sdropping, message modification	Bandwidth, data rate, throughput, Link loss rate, other link metrics
Network layer	Packet replication, routing table over flow routing table poisoning, route cache poisoning, traffic pattern distortion,	Data packet, route request, route reply, route error, TTL
Transport layer	Session hijacking, DoS, DDoS	Transmission control, congestion

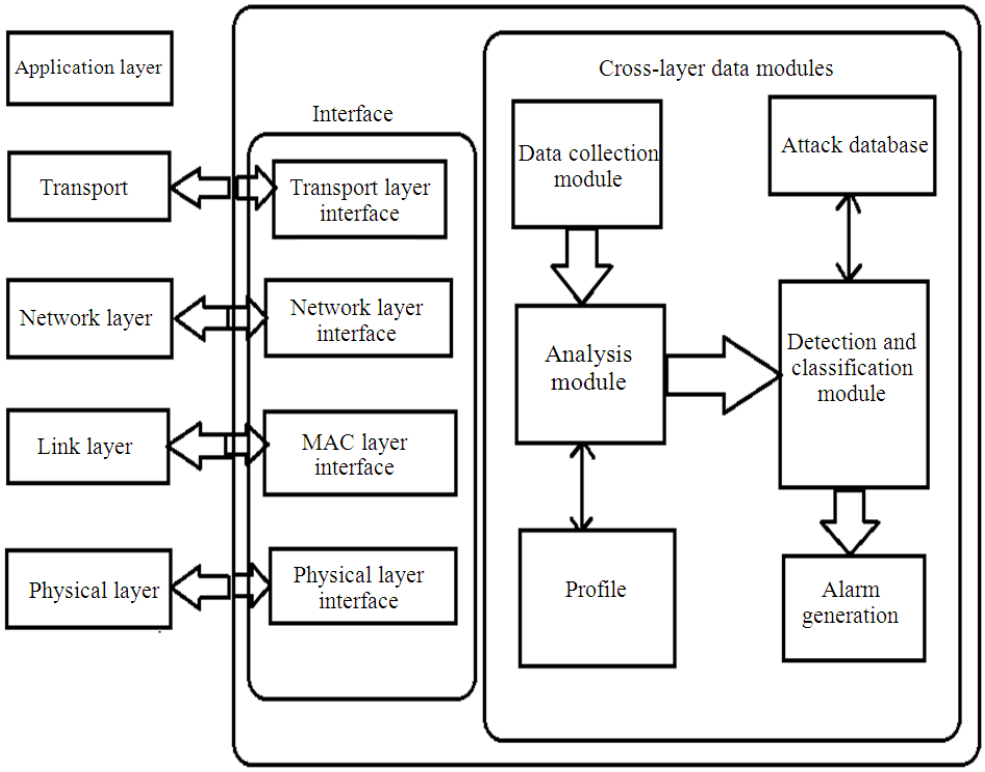

Fig. 1. Proposed crossed layer framework of IDS

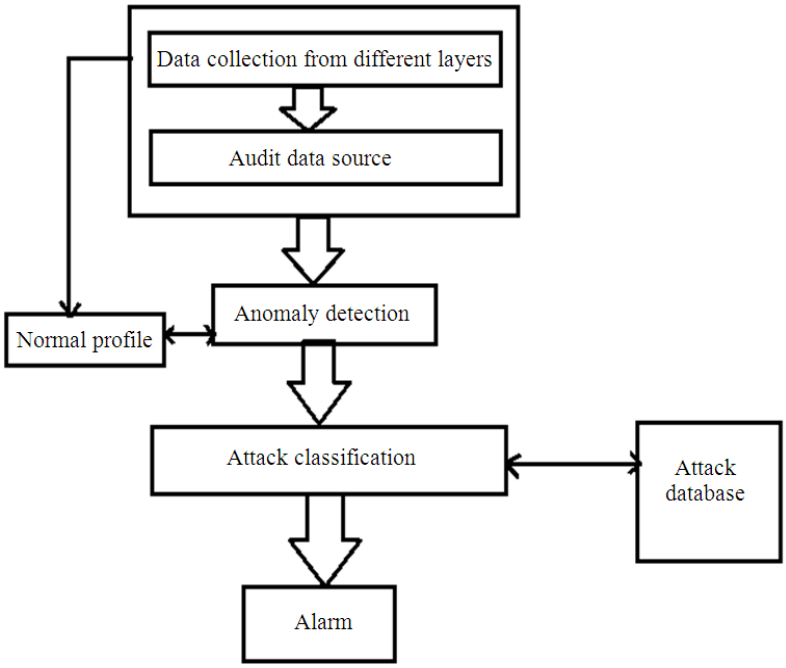

Fig. 2. Algorithm for proposed IDS

3.3.4. Method of Information Exchange

All layers work independently in the traditional protocol stack, but in case of cross layer methodology information is exchanged for optimization. Our proposed IDS is very much capable to detect several attacks by exchanging physical layer parameter in application layer and then communicate with the network layer. Data link layer and transport layer provide information to the network layer. All the parameter is calculated in the network layer **Fig. 2**.

4. EXPERIMENT

In Wireless mesh network, an attack on one layer might be affecting the performance of other layers. For example, flooding attack, having malicious node continuously sends the Synchronization packet (SYN) to every node in a network by using fake IP address to bring a network and service down. Flooding is Denial of service attack not only create network congestion, but also battery exhaustion attack which is physical layer attack. Similarly packet drop attack/Black hole attack occurs when router becoming compromised and relay packet instead of discarding. Result of a packet drop attack is end to end delay at the data link layer. So we are trying to say here, attack in one layer affect the working on another layer.

Here we generate fewer results in Network Simulator 2 (NS2) to validate a flooding attack and trying to see the effect in another layer such as congestion control in the transport layer, end to end delay in data link layer and effect on battery power in physical layer. Here we measured two metrics in our experiment:

- Detection rate (True positive rate) defines attacks are correctly measured
- False rate (False positive rate) defines abnormal behavior due to intrusion

To measure the performance of IDS we implement to attack, i.e., flooding and Black hole attack.

Our results consist of attack detection and profile training (normal network activity).Simulation parameters are given in the **Table 2**.

5. RESULTS

Here we are using the NS2 simulator and implement and lunch flooding attack **Table 3** where we send thousands of packets to the destination for congestion or service interruption **Fig. 3**.

We launched three network layer attacks, namely black holes, gray hole and routing loop attacks (Khan *et al*., 2010). **Figure 4** shows detection rate of proposed IDS in case of three network layer attacks.

We also compared the proposed cross layer IDS with a single layer IDS in the presence of different attacks **Table 4**. The single layer IDS operates in network layer only and is not capable to interact with other layers **Fig. 5**.

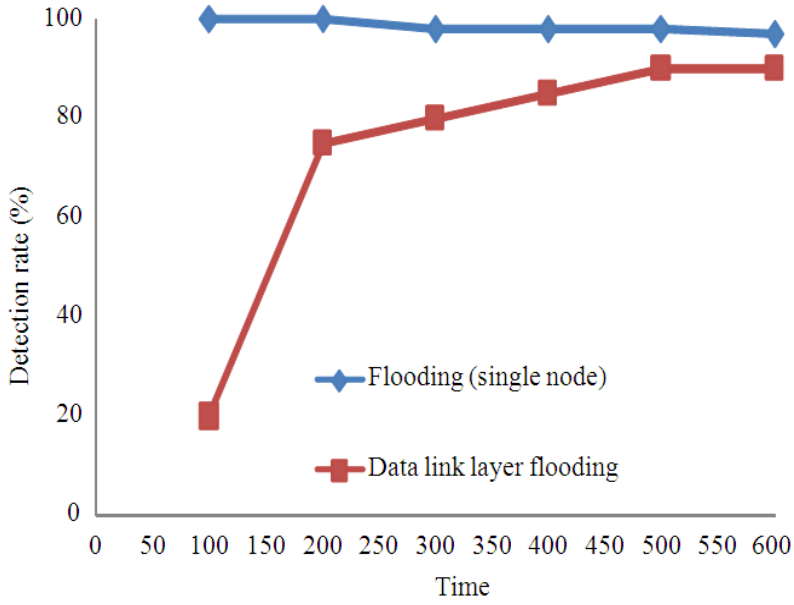

Fig. 3. Flooding attack rate

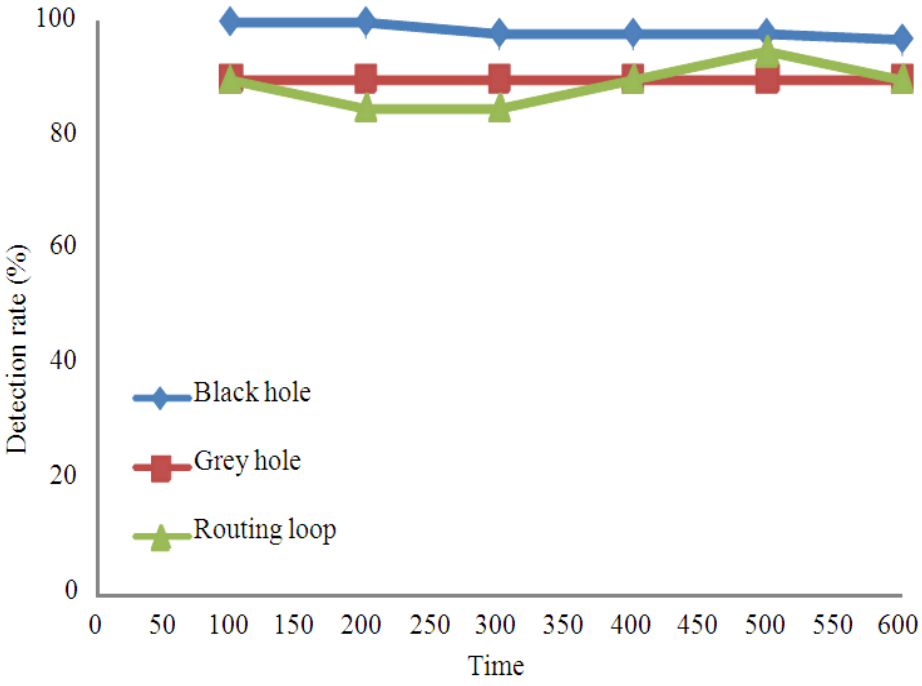

Fig. 4. Three attack detection rate

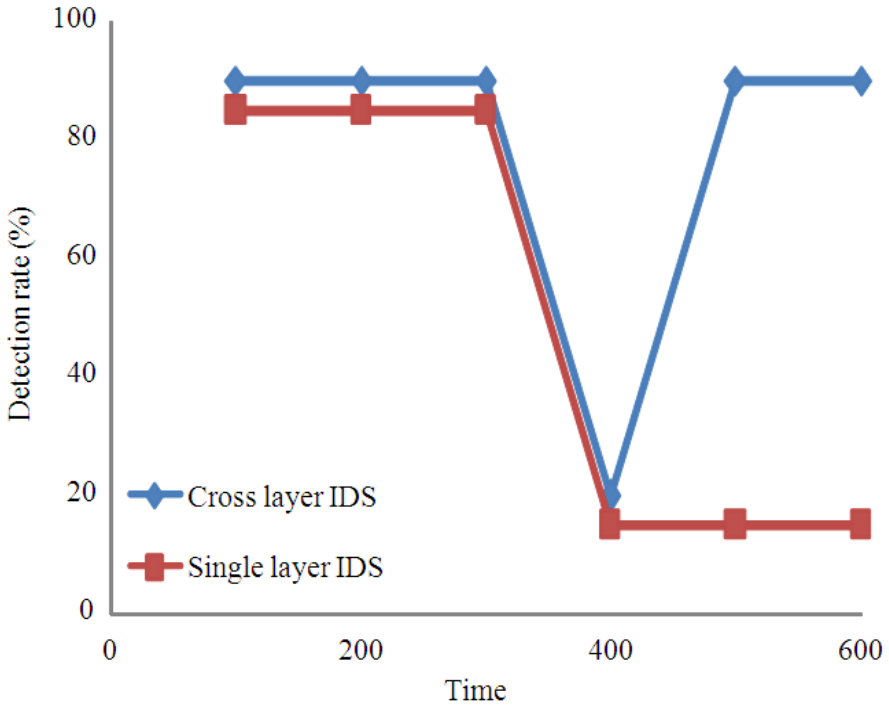

Fig. 5. Comparison of both IDSs in presence of flooding attacks

Table 2. Simulation parameters

Parameter	Value
Deployment area	600×400 m
Processor speed	Standard
Location of neighbor	Random
Radio range	20 m
Type of Battery	Standard
Normal Packet size	256 bytes
Malicious packet size	256 bytes
MAC protocol	IEEE 802.11b
Mobility	Random way point
Channel bandwidth	20 kbps
RTS	30 bytes

Table 3. Detection and false alarm rate of proposed IDS

Attack type	Rate	Alarm
Network Layer Flooding	95.8	0.5

Table 4. Detection and false alarm rate of proposed IDS

Attack type	Rate	Alarm
Gray Hole	98.0	0.3
Black Hole	97.5	0.3
Routing Loop	97.8	0.3

6. CONCLUSION

In this study, we present Cross Layer based intrusion detection system which works on a normal profile, comes from the physical layer, data link layer, transport layer and application layer. Experiments show that Cross layer intrusion detection system is more powerful than single layer intrusion detection system because single layer intrusion detection system can detect only network layer attack. Regardless of its limitations, our proposed cross layer intrusion detection system detects multiple layer attack. Our future work will focus on Jamming attack at the physical layer. We will implement such schemes which can detect unknown attacks.

7. ACKNOWLEDGEMENT

The researchers extend their appreciation to the Office of the Vice President of Research at Kuwait University. The work is completed as a part of the research project number EO 05/11.

7.1. Author's Contributions

All authors equally contributed in this work.

7.2. Ethics

This article is original and contains unpublished material. The corresponding author confirms that all of the other authors have read and approved the manuscript and no ethical issues involved.

8. REFERENCES

Boubiche, D.E. and A. Bilami, 2012. Cross layer intrusion detection system for wireless sensor network. Int. J. Netw. Secu. Applic., 4: 35-52. DOI: 10.5121/ijnsa.2012.4203

Caballero, E.J., 2006. Vulnerabilities of intrusion detection systems in mobile ad-hoc networks-the routing problem. TKK T-110.5290 Seminar on Network Security.

Chen, T.M., G.S. Kuo, Z.P. Li and G.M. Zhu, 2007. Intrusion detection in wireless mesh networks. In: Security in Wireless Mesh Networks, Zhang, Y., J. Zheng and H. Hu (Eds.)., CRC Press.

Da Silva, A.P., M. Martins, B. Rocha, A. Loureiro nad L. Ruiz *et al*., 2005. Decentralized intrusion detection in wireless sensor networks. Proceedings of the 1st ACM International Workshop on Quality of Service and Security in Wireless and Mobile Networks, Oct. 10-13, ACM Press, Montreal, Canada, pp: 16-23. DOI: 10.1145/1089761.1089765

Djenouri, D., L. Khelladi and N. Badache, 2005. A survey of security issues in mobile ad hoc and sensor networks. IEEE Commu. Surv. Tutorials, 7: 2-28. DOI: 10.1109/COMST.2005.1593277

Khalid, S. and A. Mahboob, 2013. Design and implementation of ID based MANET auto-configuration protocol. Int. J. Commu. Netw. Inform. Sec., 5: 141-151.

Khan, S. and K.K. Loo, 2009. Real-time cross-layer design for a large-scale flood detection and attack trace-back mechanism in IEEE 802.11 wireless mesh networks. Netw. Secu., 2009: 9-16. DOI: 10.1016/S1353-4858(09)70053-4

Khan, S. K.K. Loo and Z.U. Din, 2010. Framework for intrusion detection in IEEE 802.11 wireless mesh networks. Int. Arab J. Inform. Technol., 7: 435-440.

Khan, S., K.K. Loo, N. Mast and T. Naeem, 2010. SRPM: Secure routing protocol for IEEE 802.11 infrastructure-based wireless mesh networks. Springer J. Netw. Syst. Manag., 18: 90-209. DOI: 10.1007/s10922-009-9143-3

Khan, S., K.K. Loo and Z.U. Din, 2009. Cross layer design for routing and security in multi-hop wireless networks. Int. J. Inform. Assurance Secu., 4: 170-173. DOI: 10.1.1.211.7727

Khan, S., K.K. Loo, T. Naeem and M.A. Khan, 2008a. Denial of service attacks and challenges in broadband wireless networks. Int. J. Comput. Sci. Netw. Secu., 8: 1-6.

Khan, S., N. Mast, K.K. Loo and A. Silahuddin, 2008b. Passive security threats and consequences in IEEE 802.11 wireless mesh networks. Int. J. Digital Content Technol. Applic., 2: 4-8

Liu, Y., Y. Li and H. Man, 2006. A distributed cross-layer intrusion detection system for ad hoc networks. Annal. Des Télécommu., 61: 357-378. DOI: 10.1007/BF03219912

Meghanathan, N., 2013. A Survey on the communication protocols and security in cognitive radio networks. Int. J. Commu. Netw. Inform. Sec., 5: 19-38.

Northcutt, S. and J. Novak, 2002. Network Intrusion Detection. 1st Edn., Sams Publishing, ISBN-10: 0735712654, pp: 490.

Onat, I. and A. Miri, 2005. An intrusion detection system for wireless sensor networks. Proceeding of the IEEE International Conference on Wireless and Mobile Computing, Networking and Communications, Montreal, Aug. 22-24, IEEE Xplore Press, Canada, pp: 253-259. DOI: 10.1109/WIMOB.2005.1512911

Rafsanjani, M.K., A. Movaghar and F. Koroupi, 2008. Investigating intrusion detection systems in MANET and comparing IDSs for detecting misbehaving nodes. Proceedings of the World Academy of Science, Engineering and Technology, (ET' 08), World Academy of Science, pp: 351-355.

Rocke, A.J. and R.F. Demara, 2006. CONFIDANT: Collaborative object notification framework for insider defense using autonomous network transactions. Elsevier, Autonomous Agents and Multi-Agent Systems. DOI: 10.1007/s10458-005-4195-6

Shah, S.T., B. Shams and S. Khan, 2013. A survey on secure routing in wireless sensor networks. Int. J. Sens., Wireless Commu. Control, 3: 1-8.

Shrobe, H., T. Knight and A. Hon, 2007. TIARA: Trust management intrusion tolerance accountability and reconstitution architecture. Compu. Sci. Artificial Intelli. Laboratory Technical Report.

Thamilarasu, G., A. Balasubramanian, S. Mishra and R. Sridhar, 2005. A cross-layer based intrusion detection approach for wireless ad hoc networks. Proceedings of the IEEE International Conference on Mobile Ad hoc and Sensor Systems Conference, Nov. 7-7, IEEE Xplore Press, Washington, DC, pp: 7-861. DOI: 10.1109/MAHSS.2005.1542882

Wang, X., J.S. Wong, F. Stanley and S. Basu, 2009. Cross layer based anomaly detection in wireless mesh networks. Proceedings of the 9th Annual International Symposium on Applications and the Internet, Jul. 20-24, IEEE Xplore Press, Bellevue, WA, pp: 9-15. DOI: 10.1109/SAINT.2009.11