Framework for Intrusion Detection in IEEE 802.11 Wireless Mesh Networks

Shafiullah Khan[1, 2], Kok-Keong Loo[1], and Zia Ud Din[3]
[1]School of Engineering and Design, Brunel University, UK
[2]Kohat University of Science and Technology, Pakistan
[3]Gomal University, Pakistan

Abstract: *Intrusion detection system is one of the possible solutions to timely detect the intrusions and alarm for appropriate action. So far many intrusion detection systems have been proposed for ad-hoc networks, however due to the different characteristics, such intrusion detection systems cannot perform well in wireless mesh networks environment. In this paper, we propose a new framework of intrusion detection systems exclusively for wireless mesh networks. This paper will serve as a baseline guide for investigating intrusion detection systems for large scale multi-hop wireless broadband networks.*

Keywords: *Wireless mesh network, intrusion detection, and security.*

Received May 12, 2009; accepted August 3, 2009

1. Introduction

IEEE 802.11 Wireless Mesh Network (WMN) is an emerging ubiquitous broadband technology, which is going to provide and fulfil the high bandwidth requirements of end users. Unlike WLANs, WMN is proposed keeping in view the requirements of large area coverage, therefore it is also known as city-wide or community based broadband network. Large scale broadband coverage and broadband connectivity makes it more vulnerable and exposes it to different security attacks such as passive, active and Denial of Services (DoS).

The security of WMN becomes increasingly important which needs serious attention of the research community, as availability, integrity and privacy [18] are the main concerns of any secure wireless network. Several secure solutions for WMNs have been proposed by far, but most of them are prevention techniques such as authentication and encryptions which can reduce attacks, but hardly eliminate them [9].

The current rules-based and anomaly-based [7] intrusion detection systems detect intrusions either by matching patterns of network and users activities with the pre-defined rules or define normal profile of system usages, and then looks for the deviation. These approaches have their own significance and drawbacks, as the former is well suited for the known intrusions, however, it cannot detect new intrusions, while, the later relays on the deviation from the normal usage, and sometimes it even fails to detect a well known intrusion. Furthermore, WMN is exposed to multilayer security attacks.

This article analyzes some of the vulnerable characteristics and associated security attacks in IEEE 802.11 WMN. We propose a framework of Intrusion Detection System (IDS) for intrusion detection in IEEE 802.11 WMN, which is operating in hierarchical manner at two levels, i.e., lower level mesh nodes and middle level of backbone Access Points (APs).

This article presents some principal findings. First, the limitations of the existing IDS for Mobile ad hoc NETworks (MANET) and the need for exclusive IDS in WMN are discussed. Second, we propose new cooperative cross layer IDS which is capable to secure the broadband services of WMN.

2. Related Work

Being a second line of defence, IDS systems have long history. However, still it is one of the most important research issues in multi-hop wireless networks such as IEEE 802.11 WMN and MANET.

So far, many IDSs are proposed for MANET environment, which are fully explained in [1]. Watchers are used in distributed environment with link state routing protocol. These are basically used to detect network traffic based anomalies and malicious behaviour of routers. However, it needs more memory to keep records and counts of all the routers. Cooperative anomaly detection mechanisms are implemented on every node, which are independently observing their neighbours. However, if a group of nodes are compromised, they can raise an alarm against an innocent node. Watchdogs and pathraters [2, 12] are

devised for DSR routing protocol to detect network layer misbehaviours. Watchdog monitors the next hop forwarding behaviour, while pathrater analyses the results of the watchdog, and then select most reliable path for packet delivery. The scheme is limited to source routing, and cannot detect packet dropped below the threshold value particularly not effective against Invisible Node Attack (INA). Trust management Intrusion tolerance Accountability and Reconstitution Architecture (TIARA) [14] detects path failure, and each message is encrypted with digital signature, which increase its cost. Collaborative Object Notification Framework for Insider Defense using Autonomous Network Transactions (CONFIDANT) [11] monitors and rates the reputation of its neighbors, and raises an alarm in case of intrusion. However, it can mostly detect only intrusions such as packets dropping. Mobile Intrusion Detection System (MobIDS) [5] is proposed for distributed environment, in which many nodes monitors the network and sets positive values for cooperating nodes while negative value for non-cooperating nodes. The rating of nodes is broadcast to all the neighbors. However, it cannot differentiate between the real noncooperation (malicious node) and noncooperation due to some hardware failure, low battery power. AODVSTAT [15, 16] is based on AODVSTAT routing protocol. Sensors sense the radio channels, having two modes of operations. In stand-alone mode, sensor senses the attack only in its neighbours. In distributed mode, sensors periodically exchange information with the neighbours. It is a signature based approach, and how to update the attack signature files at all sensors in MANET has not been addressed. RESANE and SCAN [1], are two other approaches for multi-hop wireless intrusion detections, in which RESANE uses trust model and calculate reputations to motivate cooperation in nodes. SCAN works in distributed environment and monitors all its neighbours independently for routing and packet forwarding misbehaviour, however it is limited to AODV routing protocol. In [8, 19], the authors proposed distributed IDS for mobile nodes. However, in IEEE 802.11, most of the nodes are static. In [10], a rule based IDS is proposed, however, it is not capable to detect unknown attacks.

3. Intrusion Detection System

An intrusion is any unwanted activity either in the form of passive attacks or active attacks, which are used by the attackers to create undesired situation and harmful consequences for the user's confidentiality, network integrity or network resources availability. In simple words, any set of actions that try to compromise the data integrity, user's confidentiality or service availability can be termed as intrusion, while a system that attempts to detect such malicious actions of network or compromised nodes is called IDS [3]. However, the security level of wireless networks can be enhanced up to certain limit by implementing IDS.

The primary functions of IDS are to monitor users' activities, network behaviour and different layers. A single perfect defence is neither feasible nor possible in wireless networks, as there always exist some architectural weaknesses, software bugs or design flaws which may be compromised by the intruders. The best practise to secure the wireless networks is to implement multi lines of security mechanisms, that is why, IDS is more critical in wireless networks which is viewed as a passive defence, as it is not intended to prevent attacks, instead it alert network administrator about possible attacks well in time to stop or reduce the impact of the attack. The accuracy of intrusion detection is generally measured in terms of false positives (false alarms) and false negatives (attacks not detected), where an ideal IDSs attempt to minimize both these [1].

3.1. Classification of IDS

Two distinct types of intrusion detection systems exist. Pattern-based intrusion detection system has the capability to identify all the known intrusions, while anomaly-based intrusion detection mechanisms have the intelligence to identify and respond to new intrusions which are not known. IDS are further classified as Stand-alone IDS, Distributed and Cooperative IDS, and Hierarchical IDS [13].

Stand-alone IDS operates on each node independently to determine intrusions by monitoring the internal events which are recorded in the system logs. In distributed and cooperative IDS, every node participate in intrusion detection and response, while in hierarchical IDS, the cluster-heads monitor all of its child nodes, and respond in case of intrusion is detected.

3.2. Components of IDS

Broadly speaking, IDS has two main components [3], i.e., the features and the modelling algorithm. Features include attributes or measures which are mostly concern with the functionalities the IDS would provide. Algorithm is the core component and the efficiency and accuracy of detecting and responding intrusion is totally dependent on the underlying algorithm. IDS may have many components depend on the nature and characteristics of the network and possible intrusions. Most of the IDS have some common components such as:

- Monitoring Component, this is used for local events monitoring as well as neighbours monitoring.
- Intrusion database, which contains the records of recent misbehaviours and reputation value for the neighbours.

- Response component, which is used to respond in case of intrusion, is detected. The response may be to raise an alarm to alert the administrator or to broadcast the information to its neighbour nodes about the misbehaving node.

However, the components and the response nature of IDS is mainly dependent on the purpose and services of the IDS. For example, IDS designed for routing misbehaviour would have different components and responses as compared to an IDS which is designed for physical and MAC layers anomalies.

4. Intrusion Detection System for WMN

In the best of our knowledge, till now, there is no IDS exclusively designed for WMN. To date the existing IDS designed for multi-hop wireless networks are mostly based on the characteristics of MANET such as follows:

- Temporary network which has no support of routers and gateways; instead the nodes also perform the routing functionality.
- Application specific which is used mostly for emergency situations such as natural disasters or battle fields.
- Served by mobile nodes which posses power and bandwidth constraint.
- The traffic pattern is from users to users.

The existing cooperative and hierarchical IDS are MANET based. The entire intrusions detection and monitoring mechanisms are implemented in MANET nodes. These IDS ensures the cooperation amongst the MANET nodes to collectively monitor the intrusions and in case of intrusion found, then inform each other, or the cluster head which is responsible for intrusion detection of all its child nodes. Furthermore there is no question of involvement of the routers and gateways in MANET IDS.

As compared to MANET, the WMN has significant different network characteristics, that is why, proposing or investigating any IDS, there is a need to keep under consideration the characteristics of WMN, as well as the following important facts:

- As a large scale broadband network, WMN consists of fixed backbone mesh routers and gateways infrastructure, which is not power constraint.
- Majority of mesh nodes are static which have no power limitations; however there is also support for mobile nodes in ad-hoc and infrastructure mode.
- WMN is an integrated technology, which can enable integration amongst other wireless networks such as IEEE 802.11 WLANs, IEEE 802.16 WMANs.
- In WMN, most of the traffic is from gateway toward the nodes through static multi-hop of access points.

Keeping in view these differences, there is a need of such IDS systems which are specially designed and proposed exclusively for WMN environment. The IDS for WMN must consider its two levels i.e., end user mesh nodes and mesh routers.

Intrusions and security attacks may be possible on both lower level and middle level. The utmost need is to propose an IDS that is capable to handle the intrusions at lower and middle levels, thus we can prevent the serious disruption at the top level.

4.1. Cooperative IDS Framework for WMN

The candidate framework introduced here is cooperative cross layer IDS system as depicted in Figure 1. By adapting the fundamental operational nature of the existing cooperative and hierarchical IDS, the proposed IDS will meet the security requirement and perform well in the multi-hop, large scale, integrated broadband environment of WMN.

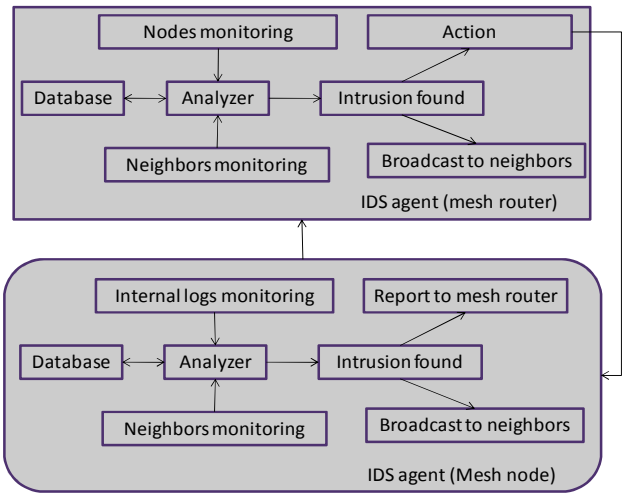

Figure 1. Framework of cooperative IDS for WMN.

The proposed IDS is keeping in view the two important levels of WMN. It is cooperative, as all the mesh nodes collectively monitor the neighbours, and inform each other if any intrusion is found, the same kind of cooperation is established at backbone mesh routers. It is also hierarchical, as it operates at two levels, i.e. mesh router is responsible to take actions against those misbehaving nodes which are in its direct communication range. In short, the proposed IDS have the following components and cooperation mechanisms.

4.1.1. IDS Agent at Mesh Nodes

Each mesh node has an IDS agent, which monitors independently its neighbour nodes, and in case of misbehaviour detection, broadcast the information to its neighbours as well as report is sent to the serving mesh router for action. It has a built-in database which has the signatures of all the well known intrusions. Furthermore, when a malicious node is detected, its information is

also stored in the database. The analyzer matches the behaviour and the signatures for detection of intrusion. The database structure is given in Table 1. The IDS agent at mesh nodes can detect routing and forwarding sorts of misbehaviours.

Table 1. Database of mesh node IDS agent.

Malicious Neighbours	Intrusion Type	Status
Node 2	Blackhole	Reported to router as well as to neighbours
Node 5	Greyhole	Reported to router as well as to neighbours

4.1.2. IDS Agent at Mesh Router

The IDS agent at each mesh router or access point has the capabilities of cross layer monitoring and detection, as IEEE 802.11 WMN is also vulnerable to many security issues at MAC layer. The parameters which the IDS agent uses for intrusion detections are listed in Table 2.

Table 2. Cross layer feature sets.

Parameters	Protocol Layer
MAC Address	Link
No. of Transmissions	Link
Time of Channel Capture	Link
Sequence Control Field	Link
TCP/IP Protocol Used	Transport, Network
Packets Analysis	Network

These parameters are helpful in identification of many attacks particularly MAC spoofing, selfishness, flooding and routing misbehaviours. The detection of probe-request flood and de-authentication attacks [4] require to counter the MAC spoofing. The 2-byte sequence control field of management frames can greatly facilitate in the regard, in which 4-bit are used for fragment number while 12-bit for sequence number [6]. The adversary either needs to control the firmware functionality or to develop a custom firmware with own source code to alter the value of the sequence control field in the management frames [17]. The IDS agent at each mesh router or access point performs some tasks such as:

- Neighbours mesh routers monitoring.
- Attached mesh nodes monitoring.
- Receive reports from mesh nodes.
- Take action against malicious nodes.

The mesh routers not only receive reports from other nodes, but also can directly detect malicious nodes. When it receive a report from mesh node regarding other mesh node misbehaviour, or it itself detect a malicious node, an action is taken against that node on the basis of severity of misbehave.

At the same time, the IDS agent of mesh router monitors independently its neighbour mesh routers, and in case of misbehaviour detection, informs the neighbour mesh routers as well as. The database structure is given in Table 3.

Table 3. Database at mesh routers.

Malicious Neighbours	Intrusion Type	Status
Router 2	Cloned	Broadcast to neighbours
Router 6	Rogue	Broadcast to neighbours
Node 8	Blackhole	Isolated (action)

The proposed algorithms for cooperative framework are given as a flowchart in Figures 2 and 3.

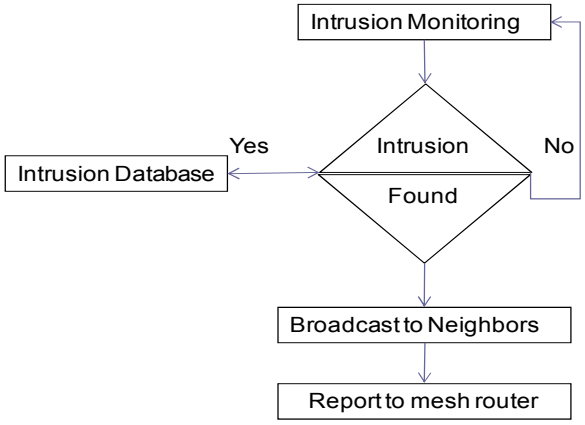

Figure 2. Proposed algorithm for cooperative IDS at mesh nodes.

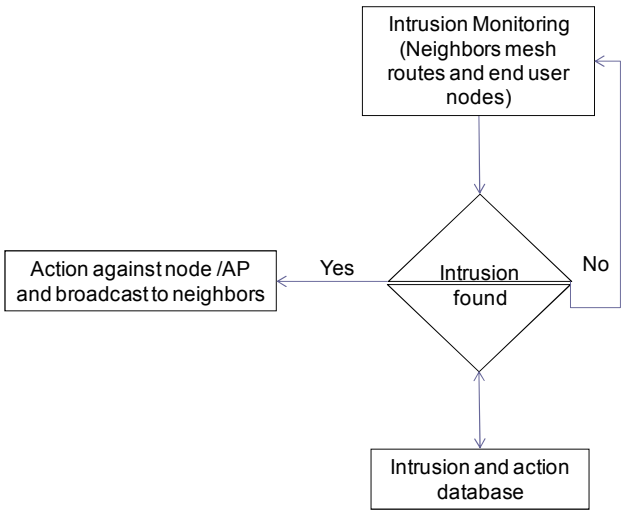

Figure 3. Proposed algorithm for cooperative IDS at mesh router/ AP.

5. Discussion

Cooperative and cross layer exclusive IDS are highly desirable for WMN keeping in view some key points.

- The proposed IDS must be cooperative in nature, as the two important components of WMN are end user

mesh nodes and multi-hop backbone of mesh routers or access points. There must be some sort of cooperation between nodes and access points so that to detect and isolate malicious nodes.

- The IDS for WMN must be cross layer, as WMN is vulnerable to multilayer security attacks, such as jamming, scrambling (physical layer), MAC selfishness and unfairness, de-authentication, spoofing attack (MAC layer), blackhole, greyhole, wormhole, jellyfish, Sybil, byzantine, flooding (network layer), SYN flood (transport layer) *etc.,*
- The IDS must have high detection rate with low false alarms. Such an IDS can perform well in the hostile environment of WMN, which is capable to detect as well as respond to intrusive activity.

6. Conclusions and Future Work

Secure communication is the key to for commercial deployment and public acceptance of new broadband paradigm of WMN. However, multi-hop WMN is vulnerable to multilayer security attacks. Some IDS systems are proposed for MANET environment; however these mechanisms cannot perform well in WMN scenario due to difference in characteristics and features. There is a need for such security mechanisms particularly IDS, which are exclusively designed for WMN environment. We proposed the cooperative cross layer framework of IDS for the hostile environment of WMN. The mesh nodes collectively monitor the neighbours and in case of intrusion found, a report is send to the mesh router for action. The mesh router takes an action against the malicious node on the basis of severity. The mesh routers also collectively monitor the neighbours for intrusion, and if a malicious mesh router is found, information is broadcast to all the neighbours. Such cooperative and cross layer IDS are indeed necessary for large scale multi-hop wireless broadband networks especially for IEEE 802.11 WMN. Our future work is to design intrusion signatures, cross layer parameters exchange to detect and respond to malicious nodes in WMN.

References

[1] Chen M., Kuo S., Li P., and Zhu M., *Intrusion Detection in Wireless Mesh Networks*, CRC Press, 2007.

[2] Caballero J., "Vulnerabilities of Intrusion Detection Systems in Mobile Ad-hoc Networks: The Routing Problem," *in Proceedings of TKK T-110.5290 Seminar on Network Security*, Japan, pp. 1-2, 2006.

[3] Djenouri D., Khelladi L., and Badache N., "A Survey of Security Issues in Mobile Ad-hoc and Sensor Networks," *Computer Journal of IEEE Communications Surveys and Tutorials*, vol. 7, no. 4, pp. 1-15, 2005.

[4] Khan S. and K., "Real Time Cross Layer Design for Large-Scale Flood Detection and Attack Trace-Back Mechanism in IEEE 802.11 Wireless Mesh Networks," *Computer Journal Elsevier Network Security,* vol. 2009, no. 5, pp. 9-16, 2009.

[5] Kargl F., Klenk A., Schlott S., and Weber M., "Advanced Detection of Selfish or Malicious Nodes in Ad Hoc Networks," *in Proceedings of 1st European Workshop on Security in Ad-Hoc and Sensor Networks*, CA, pp. 353-362, 2004.

[6] Malekzadeh M., Ghani A., Zulkarnain A., and Muda Z., "Security Improvement for Management Frames in IEEE 802.11 Wireless Networks," *International Journal of Computer Science and Network Security*, vol. 7, no. 6, pp. 68-178, 2007.

[7] Northcutt S. and Novak J., *Network Intrusion Detection*, SAMS Publishing, 2002.

[8] Oleg K. and Ratan G., "Intrusion Detection Using Mobile Agents in Wireless Ad-hoc Networks," *in Proceedings of IEEE Workshop on Knowledge Media Networking*, Japan, pp. 85-88, 2002.

[9] Ping Y., Xinghao J., Yue W., and Ning L., "Distributed Intrusion Detection for Mobile Ad-hoc Networks," *Elsevier Journal of System Engineering and Electronics*, vol. 19, no. 4, pp. 851-859, 2008.

[10] Puttini S. and Percher M., "A Modular Architecture for Distributed IDS in MANET," *in Proceedings of the International Conference on Computational Services and its Applications*, Canada, pp. 8-21, 2003.

[11] Rocke J. and Demara F., "CONFIDANT: Collaborative Object Notification Framework for Insider Defense using Autonomous Network Transactions," *Computer Journal of Elsevier, Autonomous Agents and Multi-Agent Systems*, vol. 12, no. 1, pp. 187-202, 2006.

[12] Rafsanjani K., Movaghar A., and Koroupi F., "Investigating Intrusion Detection Systems in MANET and Comparing Idss for Detecting Misbehaving Nodes," *in Proceedings of World Academy of Science, Engineering and Technology*, Canada, pp. 123-128, 2008.

[13] Siddiqui S. and Hong S., "Security Issues in Wireless Mesh Networks," *in Proceedings of IEEE International Conference on Multimedia and Ubiquitous Engineering*, Korea, pp. 178-182, 2007.

[14] Shrobe H., Knight T., and Hon A., "TIARA: Trust Management Intrusion Tolerance Accountability and Reconstitution Architecture," *Computer Science and Artificial Intelligence Laboratory Technical Report*, 2007.

[15] Tseng Y., Balasubramanyam P., Ko C., Limprasittiporn R., Rowe J., and Levitt K., "A

Specification-Based Intrusion Detection System for AODV," *in Proceedings of the 1st ACM Workshop on Security of Ad Hoc and Sensor Networks*, NY, pp. 1987-1997, 2003.

[16] Vigna G., Gwalani S., Srinivasan K., Royer Belding M., and Kemmerer A., "An Intrusion Detection Tool for AODV-Based Ad Hoc Wireless Networks," *in Proceedings of 20th IEEE Annual Computer Security Applications Conference*, USA, pp. 47-63, 2004.

[17] Wright J., "Detecting Wireless LAN MAC Address Spoofing," http://home.jwu.edu/jwright /papers/wlan-mac-spoof.pdf, 2003.

[18] Xing F. and Wang W., "Understanding Dynamic Denial of Service Attack in Mobile Ad Hoc Networks," *in Proceedings of IEEE Military Communication Conference*, UK, pp. 145-149, 2006.

[19] Yongguang Z. and Wenke L., "Intrusion Detection System in Wireless Ad-Hoc Networks," *in Proceedings of the 6th International Conference on Mobile Computing and Networking*, Canada, pp. 2926-31, 2000.

Shafiullah Khan is a PhD researcher in the School of Engineering and Design, Brunel University, UK. He is also affiliated with the Institute of Information Technology, Kohat University of Science and Technology, Pakistan as a lecturer. His research mainly focuses on wireless broadband network architecture, security and privacy, security threats and mitigating techniques.

Kok-Keong Loo received his MSc and PhD at University of Hertfordshire, UK in 1998 and 2003, respectively. Currently, he serves as a course director for MSc digital signal processing and heads a team of 9 active PhD candidates in the area of multimedia communications. His current research interests include visual media processing and transmission, digital/wireless signal processing, and wireless/broadband network architecture, protocols and securities.

Zia Ud Din received his MSc at University of Peshawar. He is serving as a lecturer in Gomal University, Pakistan. His research mainly focuses on algorithm analysis, wireless networks, operating systems, and microprocessors.