Jason Li

Professor McNair

EE 584-WS

11 November 2023

Efficient Intrusion Detection System Model in Wireless Mesh Network

Wireless Mesh Networks (WMNs) have nodes that are interconnected with other neighboring nodes which are self-organizing and self-healing. Network operations can become resilient and robust should any number of nodes fail as the data can travel a different path through other nodes. WMNs can also be reconfigurable and flexible meaning that networks can be ever growing or shrinking. Mesh networks can be constructed so all nodes are interconnected, some nodes are connected or include access points or gateways to bridge the gap to wired internet. Having all nodes interconnected would be feasible in smaller networks whereas only having select nodes interconnect could be implemented in a larger network. Various mesh network protocols include Optimized Link State Routing (OLSR), Zigbee, and Thread. OLSR uses initiative-taking link state routing which diagrams the node connections of the whole network and calculates what would be the most optimal path. This routing protocol is best for large-scale network deployments with stable topologies. Zigbee is a home and industrial automation protocol that can form energy and data-efficient self-healing mesh networks for devices with limited resources. Thread offers reliable and secure communication for (Industrial) Internet of Things (IoT) devices. Routing can be difficult in mesh networks due to the ever-changing size requirements that exist from nodes connecting and disconnecting from the system. Mesh networks also must be careful where nodes are hierarchical and how performance is affected by network size and interference. This can be managed by centralizer controllers which dictate how the network will be structured. Mesh networks also must deal with energy efficiency, and this is managed by low-power modes and sleep schedules. Automation can be implemented to ensure packets find the best route forward.

Intrusion detection systems monitor packet data traffic in a network for suspicious activities and security breaches. Unauthorized access, devices, and attacks can be detected and dealt with based on deviations in traffic data or by comparing them with a database of attack pattern data. Real-time alerts allow system administrators or security center operationalists to respond by blocking or isolating the threat, dropping malicious packets, or triggering automated scripting. These events and incidents can then be logged for further analysis and compliance reporting. Network intrusion detection systems follow this pattern and are deployed at key network points, such as firewalls and routers. Host-based intrusion detection can be installed on standalone devices like servers and workstations to monitor activity and detect unauthorized access or malware. Wireless intrusion detection investigates activity spikes that are unique to wireless networks. Intrusion detection can identify threats early and reduce downtime and server disruptions. Intrusion detection can also result in enhanced compliance due to its logging capabilities. However, intrusion detection can push false alerts due to improper configuration leading to used resources. This is further complicated by the amount of planning and updating which must be pushed through the system which can impact network performance and may require special hardware. To remedy these challenges, intrusion detection signatures, rules, and anomaly detection can be updated to optimize the system at large. Intrusion detection can also be paired with other security incident event managers to provide a layered defense.

Researchers from the Beijing Electronic Science & Technology Institute document how a proxy-based Intrusion Detection System (IDS) inspired by a Hierarchical Proxy-based Topology (HTP) structure can be implemented by designing workflows centered on two new node types: Proxy and Central Console nodes. Better security can also be adopted by grouping efficient multi-level hierarchical topology structures. WMNs in the traditional sense carry a lot of data and bandwidth at a remarkably high speed. Compared to an Ad hoc network, WMNs have self-organization, multi-hop, and high capability features that are hard to implement when a network grows. Multi-hop wireless channels are vulnerable through forging, distorting, and retransmitting information, and data as well as through (Distributed) Denial of Service (DDoS) attacks. Passive attacks can also be affected which can be remedied by encryption and security protocols, specifically IDS and firewalls. Firewalls are interesting in WMNs as they are placed to protect wireless networks which makes it quite easy for perpetrators to invade once the firewall is breached. Instead, intrusion detection has been recommended for wireless networks after some adaptations from its applications in the wired network space [1].

Research on integrating Intrusion Detection into Wireless Mesh Networks is minimal due to the new field. Distributed intrusion detection systems were investigated for Wireless Local Area Networks (WLAN) which can be potentially scaled to WMANs. Researcher Xiao Yan developed a WLAN model that integrated a Distributed Intrusion Detection System (DIDS) [2]. DIDS uses an environment that monitors multiple hosts connected to only the network. Components of DIDS include one Host Monitor per host, a DIDS Director, and one LAN monitor per LAN segment of the network. When intrusions are detected in each separate IDS, they are fed into a central hub underneath the Director via an Expert System which analyzes the intrusion data. If certain information is provided, DIDS can be utilized as an auditing tool. The

Host Monitor monitors user sessions and anomalous behavior reports as well as signature attacks. It also gathers audits from the host operating system and are combed through finding notable events which it then sends to the LAN Monitor. The LAN Monitor overlooks all traffic such as used services, traffic volume, and host-to-host connections (which can be owner verified), and reports security-related services as well as rlogin and telnet connections. A communication agent in each Host and LAN Monitor shuffles data to the DIDS Director which lessens the load on each interface. The DIDS Director is the brains of architecture and via the vital Expert System infers security of each host and LAN port [3]. Another researcher Hung Guoquan pitched a distributed sensor network to use as a detection model framework to securitize WLANs with Access Points (APs) for host-based intrusion detection, but it was not stated how IDS can be integrated into the system [4]. Finally, researcher Peng Chun-yan proposed a DIDS in a WMN but was insufficient in providing node characters that can execute IDS module functions [5]. Combining the characters and IDS found in wired networks and WMANs, the researchers of the main paper created an efficient proxy-based IDS with workflows and IDS module functions.

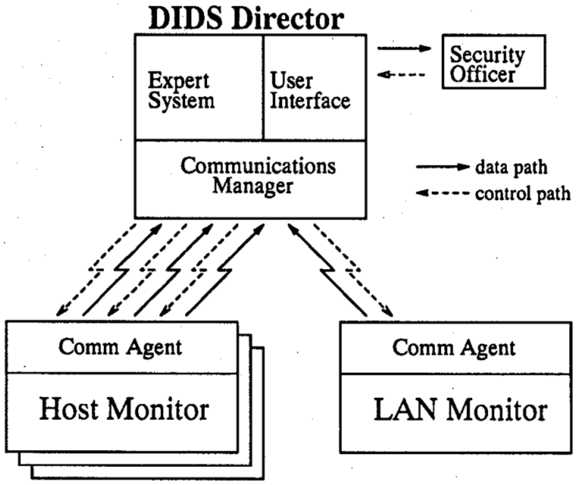

Figure 1. Distributed Intrusion Detection System (DIDS) Communications Architecture.

IDS gathers key information from various places in a computer network and investigates if any behavior goes against security regulations or fits an already documented attack pattern. This Anomaly Detection Method (ADM) is popular due to its simplicity, but threshold triggers can be difficult to implement how much traffic an anomaly results in a high False Alarm Rate (FAR). To safeguard, an IDS can prevent internal, external, and misoperation intrusions. Misuse Detection Method (MDM) utilizes descriptions of a certain mode or character to find attacking traits and system weaknesses that are stored in a database. Should the characteristics of an intrusion match the database entry, then an intrusion is considered detected. This can produce better accuracy than ADM, but it is ineffective in preventing invasions from new attack behaviors or altered known attack patterns resulting in character detection to be more stringent and frequent updates to a database.

WMNs contain many nodes; the main ones are static while others include Mesh Access Point (MAP), Mesh Portal Point (MPP, a gateway), Router, Network Server, and two new node types: Proxy and Central console. Any device can be connected as a user node while an ordinary computer or embedded equipment can be classified as a Mesh router. Compared to traditional wireless networks with gateway/bridge, WMNs have other routing protocols. The first layer of WMN is static Mesh routers that are interconnected to become a multi-hop backbone. MPP gateway nodes and APs make up the second and third layers with the latter connecting to the actual Internet. Multi-hop relays allow for bigger coverage without compromising on energy usage.

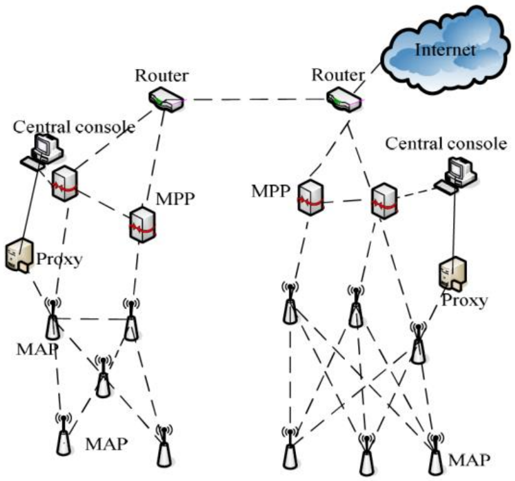

Figure 2. Wireless Mesh Network structure.

DIDs can be integrated into WMNs via distributed proxy servers where each proxy node is independent via data searching and analysis can occur within each node in software. These decisions can then be sent to the center controller that aggregates and plans intrusion detection policies for the whole network. Security can be better optimized by this self-operating principle by allowing adjacent nodes to identify system conditions, wireless communication, and user activities. Should local proxies not determine any intrusions from their evidence, it will send the reports to the gateway node that oversees executing analysis by itself or with help from other close-by proxy nodes. In simple terms, the MAP receives an access request and acts as an intermediary to a proxy node. Should an intrusion be detected, the central console will receive this alert and determine the correct course of action. If the access request is authenticated, the central console will grant access. Otherwise, the central controller will sever the wireless communication connection. No matter what the Decision-Making Module decides, the Secure Communications Module in the central console verifies the results with neighboring nodes. The MPP is then notified of the decision from the central console and the gateway can allow access through one of its ports.

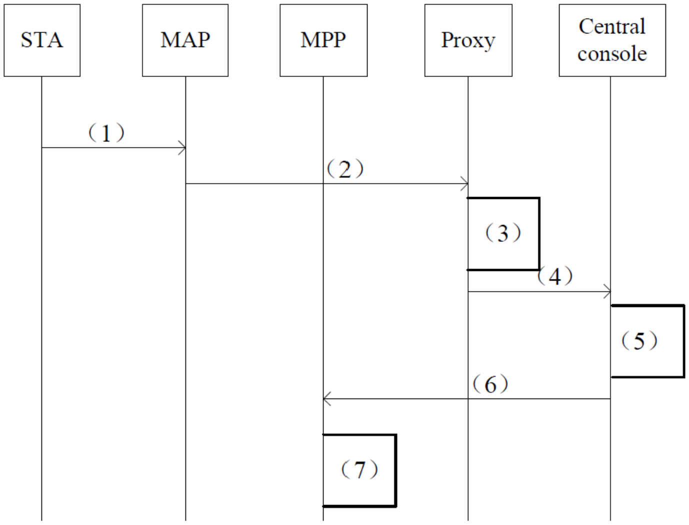

Figure 3. Working flow of proxy-based Intrusion Detection System in Wireless Mesh Network.

The Data Collection Module (DCM) audits user behavior specifically that of system and user operations, communication access action, and scope of communication. The Analysis and Detection Module (AADM) looks at pretreated data and extracts characters of data through ADM or MDM which can be combined to lessen FAR and Fail-to-Report Rate (FRR). In particular, the detection proxy-based module is most vital through wireless data package monitoring, data character identification, logging alarm information, and delivering alarm information to the central console. The Decision-Making Module (DMM) looks at the security risk of the presented intrusion and determines what proceeds next. The Management Module (MM) allows a connection to go through or disconnect from a potential user connection. The Communication Agent Module (CAM) is responsible for contacting other nearby proxies to validate the results of a proxy server that is unsure of an incoming suspicious connection.

The benefits and applications of this scheme include enhanced entity functions where these new IDS modules can be integrated into standard Mesh network architectures with low FAR and better security overall. The modular design allows for independent computation and reporting of important results to a central controller resulting in less power consumption compared to a traditional WMN. This approach is like federated learning, where machine training models are integrated into each computer and then pipes its results to a central computer. In comparison with past security intrusions, modules provide a vastly improved security experience compared to past intrusion detection systems. The hierarchical nature of this design can be upscaled to larger networks with each proxy representing a particular small region with a central data center containing a central controller that manages the mesh network. Through these means, each Hierarchical Proxy-based Topology (HPT) of networks can vary and be layered efficiently. Expansion can occur through region partitioning and sub-management consoles to lessen the load on the main central controller. Wireless Multi-hop Network (WMHN) channels are open, have limited self-stability, and have a fixed network infrastructure that presents security hurdles to overcome.

The future direction is seen as that rather than having multi-hop wireless channels and a firewall, this intrusion detection architecture on wireless mesh networks can revolutionize the way WMNs are deployed. By integrating Software Defined Networking (SDN), large networks with many nodes and routers can be better securitized by potential perpetrators. Smart home and smart city devices not only have to be energy and data-efficient but also must sustain all types of different attack vectors. With this new architecture, smart devices can be connected to proxy nodes and verified by the workflow process seen above. It also helps that smart devices can have sensors attached to give their reporting proxy nodes more details on how a device is being breached [6]. Utilizing Intrusion Detection Systems, particularly modular and topologically hierarchical ones, in Wireless Mesh Networks, is paramount to ensuring that the complete system can function and be as secure as possible.

References

[1] Y. Yang, P. Zeng, X. Yang and Y. Huang, "Efficient Intrusion Detection System Model in Wireless Mesh Network," 2010 Second International Conference on Networks Security, Wireless Communications and Trusted Computing, Wuhan, China, 2010, pp. 393-396, doi: 10.1109/NSWCTC.2010.226.

[2] Xiao Yan, Jiang Waiwen, Long Juan, "The research and design of intrusion detection system based on wireless network," *Microcomputer Information*, 2007, 23(27): 62-64.

[3] S. R. Snapp, S. E. Smaha, "The DIDS (Distributed Intrusion Detection System) Prototype," presented at the Summer 1992 USENIX, San Antonio, TX, USA, June 8-12, 1992.

[4] Huang Guoquan. Research on the IDS in Wireless Local Area Network [J]. *Science and Technology Consulting Herald*, 2007, 17:177-178 (in Chinese).

[5] PENG Chun-yan. A Distributed IDS Model Based on the Wireless Mesh Network [J]. *Journal of Gansu Lianhe University (Natural Science Edition)*, 2008, 22(2): 90-92 (in Chinese).

[6] R. Kashyap, M. Azman and J. G. Panicker, "Ubiquitous Mesh: A Wireless Mesh Network for IoT Systems in Smart Homes and Smart Cities," *2019 IEEE International Conference on Electrical, Computer and Communication Technologies (ICECCT)*, Coimbatore, India, 2019, pp. 1-5, doi: 10.1109/ICECCT.2019.8869482.