Journal of Information Systems Engineering and Management
2025, 10(53s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Layered Intrusion Detection System for Wireless Network

Ritu Rani * Rishi Pal Singh **

*Department of Computer Science and Engineering , Guru Jambheshwar University of Science & Technology, Hisar 125001 ,India
email: dahiyaritu692@gmail.com, pal_rishi@yahoo.com

*Corresponding author, Ritu Rani ; email: dahiyaritu692@gmail.com

ARTICLE INFO

Received: 30 Dec 2024

Revised: 05 Feb 2025

Accepted: 25 Feb 2025

ABSTRACT

Security in networks has become a more sophisticated problem since that such networks are open and lack infrastructure. In this paper, we describe the primary safety issues for network and data link layer protection. These levels' security needs are identified and requirements for design are established to create networks that are safe from malicious attacks. Maintaining privacy, authenticity, integrity, and non-repudiation in networked environments becomes difficult when a network architecture's security is not well planned from the beginning. This paper discusses the various attack types and identifies the security issues with intrusion detection and authentication. In order to identify nodes that aren't allowed to provide certain features, we propose a layered detection approach. Due to the distinct characteristics of wired and wireless networks, intrusion detection methods designed for wired networks are no longer appropriate or efficient when implemented onto wireless networks. The research presented here initially identifies the security issues with wireless network intrusion detection, afterward propose a framework for multilayer intrusion detection.

Keywords: Authentication, Intrusion detection, Layered security, framework.

1. INTRODUCTION

Basic network functionality like packet forwarding, routing, and network management are supported by every node that is accessible in wireless networks, as compared to networks that use dedicated nodes for these purposes. A wireless networks are collections of nodes capable of communication without the help of a predetermined framework. Nodes use wireless radios to connect with each other and perform according to the idea of a peer-to-peer network. Additionally, We refer to these networks as mobile ad hoc networks. From rapid civil development to military activities, mobile ad hoc networks are utilized everywhere, including data collection/sensor networks and emergency search and rescue missions. Because ad hoc networks are easily set up, but sensitive applications represent serious security risks. Compared to traditional wired networks, wireless networks have various security requirements. Because mobile devices have limited technical capabilities, the fundamental security needs the availability, confidentiality, integrity, authentication, and non-repudiation. (such as low-power microprocessors, limited memory and bandwidth, and minimal battery life and changes in the configuration of the network, they are seen differently for networks. This article focuses on identifying security risks and vulnerabilities in the networks, as well as analysing secure protocols in the network and data connection levels.

The wireless network's nature makes it accessible to malicious attacks from an adversary. These networks are vulnerable to assaults that range from active interference to passive eavesdropping. Every node in a wireless network can be the target of attacks which originate from any direction , in comparison with physical networks where an attacker need to physically enter the network or bypass many safety features at firewalls and gateways. Additionally, the lack of a centralized power allows adversaries to breach the cooperative algorithms required for effective operations and to leverage new kinds of attacks.

In our paper, we propose a layered intrusion detection system for wireless networks' hostile nodes. It is made possible by the main networking functions, which are data packet forwarding and routing at the network layer and the open system interconnection (OSI) link layer with one-hop connectivity and frame transmission. We suggest a two-phase detection process the primary functions of ad-hoc networks enable detection framework, that are present at the network or data link layer. The suggested system model's depend on zero knowledge approaches that have been created especially to identify nodes without the usage of digital signatures, sequence numbers, timestamps, symmetric or asymmetric encryption algorithms, or any of these. We look at secure protocols in the network and data connection levels and try to identify security vulnerabilities and attacks in these kinds of networks. Furthermore, we propose a layered security architecture that employs several defences against malicious attempts and other network faults.

After this introduction, the paper is organized as follows. Section 2 describes the intrusion detection difficulties and also discusses data link layer and security features of data link and network layer security mechanisms, as well as the difficulties they provide in securing networks, are presented by network layer challenges. In section 3, we presents layered security model and also discusses the detection framework. Section 4 describes validation procedure of layered model . At last, a summary of our contribution and recommendations for further study in the work conclude in Section 5.

2. IDS CHALLENGES

Usually, the first line of security is an intrusion prevention technology like authentication and encryption when several types of activities occur with the intent to put at risk a system's availability, confidentiality, or integrity. However, as systems grow more complex and security is sometimes considered an afterthought, intrusion prevention by itself is insufficient. Errors in code and design, as well as other socially engineered penetration techniques, inevitably cause vulnerabilities in the system. For instance, some recently released system software still has vulnerable "buffer overflow" security flaws that might result in an unauthorized access shell, despite the fact that these flaws were first discovered several years ago. Additionally, As shown by the distributed denial-of-service assaults against well-known websites that have security safeguards in place, networks and protocols built to provide services are inevitably open to DDoS attacks. Since a reaction must be implemented for minimizing damages as soon as an attack is identified, intrusion detection must be operate as a backup defence of protection for systems security. By definition, intrusion detection includes collecting information and analysing the evidence to ascertain whether the system is being attacked [1,8,30,9,10,11]. In comparison with wired networks, which typically use switches, routers, hub and gateways for traffic monitoring, NIDS (Network-based IDS), Since wireless network system excludes these traffic concentration sites, it belongs to host-based intrusion detection systems.

While host-based IDSs are focused on what is occurring on every single node, network-based IDSs examine all network traffic [8,9,10]. They usually work by examining log files or keeping an eye on real-time system activity, and they can identify updates to important system files or repeated unsuccessful access attempts. Furthermore, in a network, it could be difficult to differentiate between normal and abnormal. If a node sends incorrect routing information, it could be compromised or simply momentarily because of abnormal activity. Several security-related research on detection techniques for wireless networks depends upon infrastructure, including [1,8,9,10,11]. To ensure the reliability and correctness of routing data, general preventative strategies like key creation and management has been applied in a distributed way [2,3,4,12].

Zhou and Haas [7] a distributed key management service was introduced that is independent of the routing protocol. This method provides reliable key management through the use of redundancies in the network topology. The primary concept is utilizing key sharing even when the ratio of compromised nodes to total nodes reaches a certain threshold. The challenges in implementing each of such strategies are: First, the cost of cryptography on hosts is really expensive ,where there is relatively limited computational capability; Second, because there doesn't seem a reliable central authority, It is more challenging to implement authentication; Third, these methods are ineffective when an internal node has been compromised and only useful for preventing from external attacks. Given that cryptographic methods are mainly used to perform system authentication, designing effective techniques for achieving reliability without resorting to digital signatures, encryption techniques, etc., is important.

2.1 Challenges with the data link layer

When component in the Open Systems Interconnect program, For creating computer network protocols and communications, interconnection reference model for open systems is a multi-layered abstract description. Second layer of the OSI model's, data link layer, is responsible for ensuring that data is accurately transported among nearby network nodes. For data transfer between network entities, the data link layer offers both procedural and functional tool for detecting and may be resolving any physical layer errors. However, frame transmission and one-hop connectivity are the primary link layer functions associated with ad hoc networking [13]. Data link layer protocols maintain the accuracy of frames delivered and maintains communication between nearby nodes.

It is important to determine the applicability of safety measures put in place at the data connection layer in relation for the needs of a secure network. Both the surroundings that are both trusted and untrusted environments exist in mobile ad hoc networks [22,26,20,29,27]. With a trusted environment, wireless network's nodes are under the direction of a third party and are therefore reliable due to authentication. In this case, the necessity of establishing a reliable infrastructure using logical security techniques justifies data layer security. If it's possible to ensure that the trusted nodes' implementation of the higher layer functions, therefore the security parameters produced by further layers, such as procedures for application protocols and routing, can even be met by data link layer security.

However, in non-trusted environments, data connection layer security techniques cannot be used to establish confidence in upper levels including application protocols or routing. Data integrity and authentication from node to node, which are necessary for the routing layer, seem to be the only relevant applications of the latter. Furthermore, automated key management support is not sufficient that is essential in open areas where installing keys manually is inappropriate—is primary barrier to the implementation of current data connection layer security measures.

The primary need of data connection layer security measures to address absence of physical safety on the communication infrastructure's wireless segments. According to WEP's 802.11 objectives the data connection layer may be viewed as a way to build a security that is "wired equivalent". The main purpose of data link layer methods, such as those offered by Bluetooth and 802.11, is to improve privacy and regulate access in order to address the weaknesses regarding radio communication connections. Still, data connection safety features implemented at every hop is unable to satisfy applications' end-to-end security needs, nor can it be applied to IEEE 802.11-protected wireless communications or neither Bluetooth nor physically secured wired connections. Recent studies have identified weaknesses in WEP, and misuse of the cryptographic primitives can result in a variety of cryptographic attacks [15]. Additionally vulnerable to DoS attacks, the IEEE 802.11 protocol allows an adversary to use the back-off of its binary exponential mechanism to prevent its immediate neighbours from accessing the wireless channel. Furthermore, a node that transmits continually has the ability to obtain channel, causing other nodes to back off indefinitely, which sets off a series of events from protocols at the top layer like management of TCP windows. Using , the channel reservation is specified by the NAV field in the request to send or clear RTS/CTS frames, IEEE 802.11 is also susceptible to another DoS attack. The adversary may purposefully use wireless interference to add a 1-bit error into the link layer frame of the victim after overhearing the NAV information [22,15]. By optimizing crucial security processes such frame encryption, integrity of data checking, node availability, and node verification, link layer security protocols should enable secure frame transmissions and peer-to-peer security for nodes that are directly connected.

2.2 Challenges with the network layer

In seven-layer OSI model, network layer is the third layer. In along with addressing messages, the network layer translates names and converting logical addresses to physical addresses. Additionally, it manages traffic issues including switching, routing, and regulating data packet congestion in addition to figuring out the route from the starting computer to the recipient computer. Data packet forwarding and routing are the two primary network functions associated with ad hoc networking [16,25]. According to the routing data, the routing protocols preserve the routing states at every node to exchange information between nodes. Data packets are routed to their destination by intermediate nodes along a predetermined path based on the routing states.

Attackers can use compromised nodes to generate traffic towards specific destinations and forward packets along an inefficient path by exploiting routing protocols. Additionally, the adversaries have the ability to generate channel contention, network congestion, and routing loops in certain regions of the network. Research into detecting and thwarting increasingly complex routing attacks is still occurring[28,18] . The attacker may initiate attacks against packet forwarding activities in in addition to routing. These types of attacks result in the delivery of data packets that deviates from the routing states. In some cases, the attacker could duplicate the packets it has already transmitted, change their content, or drop the packets along a known path [29]. Another kind of attack is denial-of-service (DoS),which attacks packet forwarding mechanisms and produces network and wireless channel contention in mobile networks [26,20,27].

Routing protocols are categorized as proactive, reactive, or hybrid protocols based upon network framework[23]. Distance vector or table-driven protocols are examples of proactive protocols. To ensure that each node can function instantly with consistent and current routing database, the nodes in these protocols frequently update the current routing information [23]. On the other hand, the routing information is not updated on a regular basis by reactive or source-initiated on-demand protocols [19]. Consequently, they incur significant overhead while determining the route because the routes aren't always updated when needed. Hybrid methods combine proactive and reactive approaches. Usually, they provide the ability to dynamically change between the protocol's reactive and proactive modes [19]. Reactive routing strategies like dynamic source routing and ad hoc on-demand distance vector are the primary focus of current research to develop secure routing mechanisms [24,14], that have been established to be better than the proactive ones while having substantially reduced overheads. When topology changes are less frequent, they can respond rapidly to them while maintaining a low routing overhead during specific times or in specific parts of the network.

Current literature-proposed secure routing methods account for active attacks carried out by compromised nodes that aim to have an effect with routing protocol execution, On the other hand, passive attacks and concerns of selfishness issues are left unaddressed. Such as, the reactive protocol for secure routing [16,25] ensures that the appropriate topological information is obtained. According to the parties' public keys involved in communication, A hybrid key distribution is used. However it faces obstacles by the absence of a route upkeep message method of validation [29,21]. An additional secure reactive ad hoc routing system depend upon DSR, ARIADNE, secures point-to-point confirmation through the use of a shared secret key and a message authentication code [25,17]. In an ad hoc setting, the secure routing protocol ARAN identifies and guards against unauthorized activities by peers and outsiders parties. It prevents against exploits that use impersonation, fabrication, and modification because it uses asymmetric cryptography, it is an extremely expensive protocol in terms of power and CPU utilization. The use of an alternative protocol defeats the wormhole attack [25]. On the other hand, SEAD is a proactive technique that addresses attackers who change information about routing . It depends on the protocol for destination sequenced distance vectors [17]. Effective one-way hash functions are used instead of costly asymmetric cryptography techniques. Since SEAD is unable to manage wormhole attacks, the authors suggest using an alternative protocol, similar to the ARIADNE protocol, to identify this specific threat [18].

3 LAYERED SECURITY DESIGN

Since existing wireless network proposals first identify a number of security problems and then either improve current method or suggest a new one to counter those attacks, they are usually attack-oriented. The solutions function effectively when specific attacks are present since they are specifically created with specific attack models in mind, but they may not withstand novel attacks. It is challenging to accomplish the aforementioned security objectives during network deployment when a network architecture's security is not appropriately planned from the start. Therefore, it becomes essential to create secure networks that will provide several ways to defend against known and undiscovered attacks. Layered security design is the term for this type of design.

In the design of the multi-layered security, we consider operational failures, severe network overload, and misconfigured networks in addition to malicious attacks. From a network and end-user perspective, all of these errors, whether carried on by assaults or configuration errors, exhibit certain symptoms and ought to be managed by security measures. Furthermore, the system as a whole be robust without being impacted by the failure of any one line of defence.

one- hop

connectivity-Frame Transmission

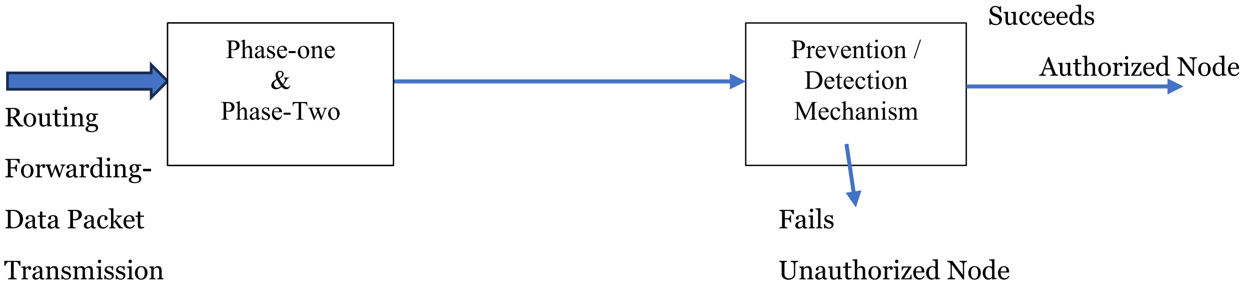

Fig. 1 Prevention / Detection framework.

As mentioned above, In wireless networks, the existing proposals are detection-oriented or authentication-oriented as it initially recognize existing weaknesses before either proposing a new method to counter such attacks or improving the current protocol. Because the solutions were specifically developed with specific attack models in consideration, they perform effectively when specific attacks are present but may not withstand emerging attacks. The detection framework we suggest is connected to a network's primary functions, those can be identified in the reference model for open systems interconnection's link and network layers, as shown in Fig. 1(OSI). The primary functions involved with networking, routing and data packet forwarding in network layer, and one-hop connectivity and frame transmit in data link layer[5,6,7]. While routing protocols communicate maintaining routing states at each node and transferring information across nodes appropriately, Data link layer protocols ensure neighbouring nodes' connectivity and guarantee the accuracy of data packets delivered. The intermediary nodes send data packets along a specific route to the destination based on the routing states.

These procedures include network and link security techniques that incorporate two-phase detection system. These phase detection mechanisms use a non-interactive zero knowledge protocol to identify unauthorized nodes by attempting to ascertain the real identity of the communicating nodes. When any malicious intruder joins the network and becomes successful in isolating any system, link failure occurs, which makes the whole path disconnected. There are also high chances that the malicious intruder compromises any good system and they also behave like a malicious intruder. This phase detects the unauthorized node when systems or any new user are introducedin the network architecture for the first time. These nodes must be authenticated and their identity must be checked properly before giving them all rights and privileges to access the network resources. Because they are highly prone to malicious attacks and can sabotage the whole architecture. In Figure 2, let's say that A, B, and C are all authenticated systems. When system X1 wants to connect to the network, it has to be authenticate by authenticated systems.

Prevention, detection, and reaction operations should all be part of the layered security measures to keep attackers out of the network. They should to identify the intrusions and take steps to stop any long-term negative impacts. Protocols for packet forwarding and secure routing may include the prevention procedure to stop attackers from installing improper routing configurations on nodes.

3.1 Detection Procedure for detecting unauthorized nodes

As explained in challenges with data link layer security, network layer functions like forwarding of data packets and routing, link layer functions include one-hop connectivity and transfer of frames. Link as well as network safety techniques which incorporate a procedure for protocol security are included in these operations. By identifying anomalous behaviour by malicious participants, the detection mechanism takes advantage of ongoing attacks. Node availability techniques or node-to-node authentication can both identify such misbehaviour.

Figure 2 illustrates validated A, B, and C system. System X1's join the network, as shown in Fig. 2, It will be validated by nearby systems that are B and C. Due to the establishment of new routes between nodes, when two nodes, such as X1 and X2, join the network, their neighbours will validate them both. For example, node X1 is verified as an authentic node by the nearest nodes, making system X1 a valid system. In a similar way the most nearby system X2 will be authenticated by systems B and X1 upon its arrival in the network. Nodes X1 and X2 will authenticate one another after being verified by valid nodes because they will be the ones who transmit and receive routing and packet forwarding data.

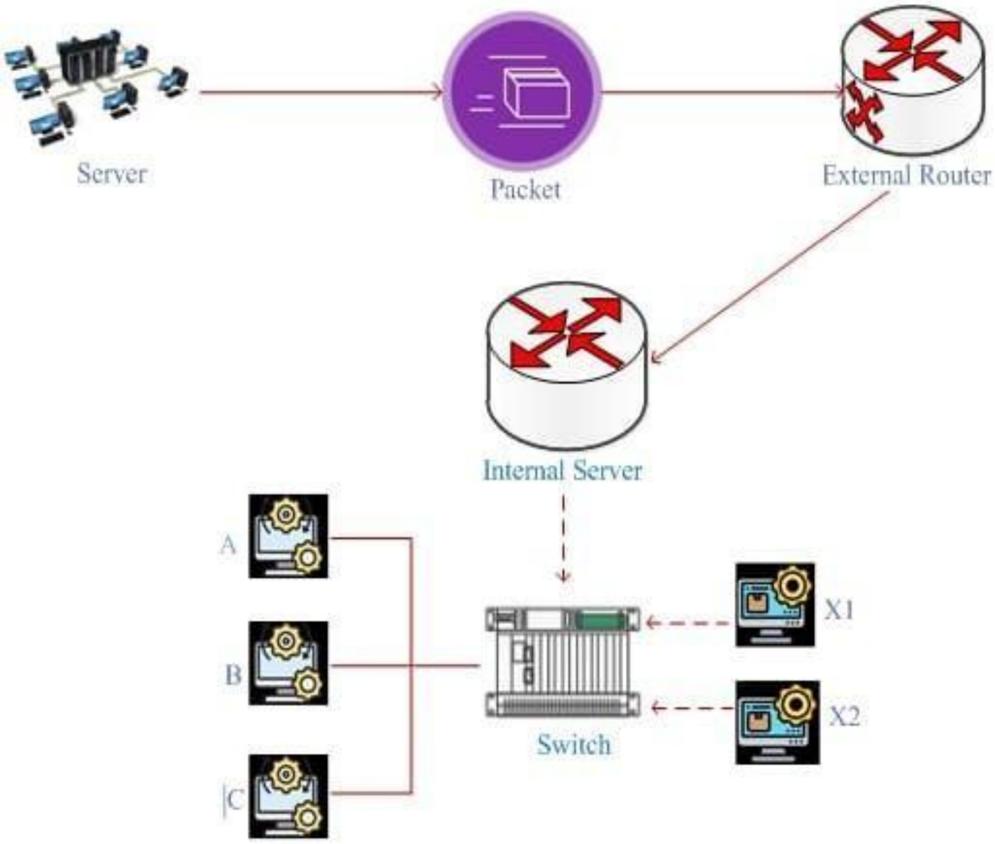

Fig. 2. New nodes in Network

The literature provides a number of authentication protocols that can be used with networks. But in order to avoid more computational burden to the network, non-interactive, low-complexity protocols need to be used. As an example, in phase one, a verifiably reliable authentication technique could be regarded as "good" alternative. Such an approach is better than an authentication scheme that is computationally secure. Since its security depends on a well-known computer problem's seeming intractable nature and does not always need a method of encryption that is either symmetric or asymmetric. Therefore, a zero knowledge protocol [18], which offers these features, can be implemented for authentication. The fundamental premise behind the usage of these cryptographic methods is that, even in cases where the claimant node misbehaves, they enable an applicant, or node within a network, to show that you are aware of a secret while disclosing no information that would be useful to the verification node. These protocols, which are also known as interactive protocols, require nodes to exchange many messages; the evidence is probabilistic rather than absolute.

As you can see in Fig. 2, node X1 uses this discrete procedure to prove its identity to nodes B and C $Y_1 = \beta_1{}^{x1}$ and $Y_2 = \beta_2{}^{x2}$ (to the bases β_1, β_2) ,satisfy Eq. 1

$$\kappa_1.x_1 + \kappa_2.x_2 = b \ (\mathrm{mod}\ p) \qquad (1)$$

for integers κ_1, κ_2, with the prime number p.

Following that, node X1 first calculates $Y_3 = \beta_3{}^{x3}$ and $Y_4 = \beta_4{}^{x4}$ then resolves Equation 2 for the integers x_3, x_4.

$$\kappa_1.x_3 + \kappa_2.x_4 = 0 \ (\mathrm{mod}\ p) \qquad (2)$$

The exchange of messages that followed then proceeds :

$X1 \rightarrow B,C : Y_5 = \beta_1{}^{x3} \qquad Y_6 = \beta_2{}^{x4} \qquad (M1)$

B,C sends message X1 after computing Y_7 using a one-way hash method.

$B,C \rightarrow X1 : Y_7 = H (\beta_1, \beta_2 ,Y_1 ,Y_2 , \kappa_1, \kappa_2 ,b, Y_5 ,Y_6) \qquad (M2)$

Node X1 creates a message (M3), verifies the authenticity of M1 and Y_8, Y_9, are sent to nodes B and C.

$X1 \rightarrow B , C : Y_8 = x_3 - Y_7.x_1 \text{ (mod p)} ,$

$Y_9 = x_4 - Y_7.x_2 \text{ (mod p)}. \qquad (M3)$

Node X1 proves to systems B and C that is aware with discrete method of Y_1 and the logarithms satisfy a linear equation to the bases of β_1 and β_2. It can be finished through examining out the final showing (Y_7 ,Y_8 ,Y_9). It is always possible for B and C to generate a legitimate verification by initially reconstructing.

$$Y_{10} = \beta_1 Y8 . Y_1 Y_7$$

$$Y_{11} = \beta_2 Y_9 .Y_2 Y_7$$

B, C validate that X1 is who he is and determine whether Y7 equals Y12 or not.

In the above

$H (\beta_1, \beta_2 ,Y_1 ,Y_2 , \kappa_1, \kappa_2 ,b, Y_{10} ,Y_{11}) = Y_{12}$

Whenever equation 3 is correct, then:

$$\kappa_1 .Y8 + \kappa_2 . Y_9 = - Y_7. b \text{ (mod p)} \qquad (3)$$

First, systems B and C may consistently succeed in creating authentic proof since

$$Y_{10} = Y_5$$

$$\text{and} \quad Y_{11} = Y6$$

$Y_{10} = \beta_1{}^{Y8} . Y_1{}^{Y7\,Y8.Y1} = \beta_1{}^{X3\text{-}Y7.X1} . \beta_1{}^{X1.Y7} = \beta_1{}^{X3} = Y_5$

$Y_{11} = \beta_1{}^{Y9} . Y_2{}^{Y7\,Y9.Y2} = \beta_1{}^{X4\text{-}Y7.X2} . \beta_1{}^{X2.Y7} = \beta_1{}^{X4} = Y6$

Therefore, in message (M2), systems B and C calculated Y_{12} will compare it to Y_7. Additionally, systems B and C check to see if responses Y_8 and Y_9 satisfy eq.(3).Hence ,

$\kappa_1 Y_8 + \kappa_2 Y_9{}^{Y8,Y9} = \kappa_1.(x_3\text{-}Y_7.x_1) + \kappa_2.(x_4\text{-}Y_7.x_2)$

$= \kappa_1.x_3\text{-}\kappa_1 Y_7.x_1 + \kappa_2.x_4\text{-}\kappa_2 Y_7.x_2$

$= \kappa_1.x_3 + \kappa_2.x_4 \text{ -Y7. } (\kappa_1.x_1 + \kappa_2.x_2)$

Equation 1 and 2 $- Y_7.$ b (mod p) and confirm Node X1's identity.

4. VALIDATION PROCEDURE FOR LAYERED SECURITY MODEL

During the confirmation process , Node X1 performs calculations $Y_3 = \beta_3{}^{X3}$ and $Y_4 = \beta_4{}^{X4}$ and as well as solving equation 2 for the numbers x_3 and x_4.

After that, the following message exchange occurs:

$X1 \rightarrow B,C : \; Y_5 = \beta_1{}^{X3}$

$Y_6 = \beta_2{}^{X4} \qquad (M1)$

$B,C \rightarrow X1 : Y_7 = H(\beta_1 ,\beta_2 ,Y_1 ,Y_2 , \kappa_1, \kappa_2 ,c ,f (a_1 ,a_2)+b, Y_5 ,Y) \qquad (M2)$

$X1 \rightarrow B, C: Y_8 = x_3 - Y_7.(f (a_1, a_2) + x1) \text{ (mod p) },$

$$Y_9 = x_4 - Y_7.(\, f\,(\,a_1,\, a_2\,) + x2\,)\ (\text{mod } p\,) \qquad (\,M3\,)$$

Validating the final proof (Y_7, Y_8, Y_9) will show that X1 convinces nodes B, C.

First B, C are reconstructing

$$Y_{10} = \beta_1{}^{y8} \boldsymbol{.}\ Y_1{}^{Y7}$$

$$Y_{11} = \beta_2{}^{y9} \boldsymbol{.}\ Y_2{}^{Y7}$$

Following that, checking if Y_7 are equivalent to Y_{12} :

$$H\,(\beta_1, \beta_2, Y_1, Y_2, \kappa_1, \kappa_2, c, b, Y_{10}, Y_{11}) = Y_{12}$$

Also, if equation 6 is correct :

$$\kappa_1.Y_8 + \kappa_2.Y_9 = -Y_7(f\,(a_1, a_2) + b\ (\text{mod } p)\,) \qquad (\,6\,)$$

For

$$\kappa_1.\ f\,(a_1, a_2) + \kappa_2.\ f\,(a_1, a_2) = 0\ (\text{mod } p) \qquad (\,7\,)$$

B and C will be able to produce reliable proof as ,

$$Y_{10} = Y_5$$

$$\text{And} \quad Y_{11} = Y_6$$

$$Y_{10} = \beta_1{}^{Y8} .\ Y_1{}^{Y7\,Y8.Y1} = \beta_1{}^{X3-Y7.(f\,(a1\,,a2\,))+X1} .\ \beta_1{}^{Y7.(f\,(a1\,,a2\,))+X1} = \beta_1{}^{X3} = Y_5$$

$$Y_{11} = \beta_2{}^{Y9} .\ Y_2{}^{Y7\,Y9.Y2} = \beta_2{}^{X4-Y7.f\,(a1\,,a2\,))+X2} .\ \beta_2{}^{Y7\,.(f\,(a1\,,a2\,))+X2} = \beta_1{}^{X4} = Y_6$$

Then

$$Y_{12} = H\,(\beta_1, \beta_2, Y_1, Y_2, \kappa_1, \kappa_2, c, b, Y_{10}, Y_{11})$$

$$= H(\,\beta_1, \beta_2, Y_1, Y_2, \kappa_1, \kappa_2, c, b, Y_5, Y_6\,) = Y_7$$

Hence , B and C calculate Y_{12} and comparison with Y_7 within the message (M2). Additionally, Nodes B, C check to see if replies to Y_8 and Y_9 fulfil equation (6).

Therefore,

$$\kappa_1.Y_8 + \kappa_2.Y_9{}^{Y8.Y9} = \kappa_1.(x_3 - Y_7.(f\,(a1,a2\,) + x_1)) + \kappa_2.(\,x_4 - Y_7.(f(a1,a2\,) + x_2))$$

$$= \kappa_1.x_3 - \kappa_1.Y_7.f\,(a1,a2) - \kappa_1.Y_7.x_1 + \kappa_2.x_4 - \kappa_2.Y_7.(f\,(a1,a2\,) -$$

$$\kappa 2.Y_7.x2$$

$$= \kappa_1.x_3 + \kappa_2.x_4 - Y_7.(\,\kappa_1.x_1 + \kappa_2.x_2) - Y_7.(\,\kappa_1.\ f\,(a1,a2) + \kappa_2.$$

$$f\,(a1,a2)\,)$$

Equation 2, 4 and 7

$$= -Y_7.(\,f\,(a1,a2) + b)\ (\text{mod } p)$$

Hence, the nodes that communicate might decide on a secret key to encrypt the transmission effectively.

5. CONCLUSION

Due to lack infrastructure and networks are inherently open, security is a more challenging issue. The most researched topic in the current hierarchical research efforts on wireless networks is secure routing networks. Routing protocols are examined more than authentication and key management techniques. Furthermore, link security protocols represent the least researched field. Thus, both data and network layers should be focus of security criteria including authenticity, confidentiality, integrity, and non-repudiation. The security needs were examined in this article using a layered approach, whereby tools for detection, prevention, and response should be available. In order to identify unauthorised nodes in networks, nodes use zero knowledge techniques to pass on information. The primary objective of research in the area of network authenticity and integrity is to design such cryptographic algorithms that are effective in message overhead and computational overhead. One of biggest challenges of wireless sensing, for example, is creating effective cryptographic techniques for key management and authentication in broadcast and multicast contexts. Existing and effective symmetric algorithms can be used to address data confidentiality and integrity problems once the infrastructure for authentication and key management is created because no specific integrity and encryption methods for networks need to be developed.

REFERENCES

[1] A. Mishra, K. Nadkarni, A. Patcha, Intrusion detection in wireless ad hoc networks, IEEE Personal Communications 11 (1) (2004) 48–60.

[2] C.M. Chlamtac, J.J.-N. Liu, Mobile ad hoc networking: imperatives and challenges, Ad Hoc Networks 1 (July) (2003) 13–64.

[3] D. Watkins, C. Scott, Methodology for evaluating the effectiveness of intrusion detection in tactical mobile ad-hoc networks, in: IEEE Wireless Communications and Networking Conference (WCNC), vol. 1, 21–25 March 2004, pp. 622– 627.

[4] E.C.H. Ngai, M.R. Lyu, Trust- and clustering-based authentication services in mobile ad hoc networks, in: 24th International Conference on Distributed Computing Systems Workshops, June 2004, pp. 582–587.

[5] J. Kong et al., Adaptive security for multi-layer ad-hoc networks, Special Issue of Wireless Communications and Mobile Computing, John Wiley Inter Science Press, 2002.

[6] L. Blazevic et al., Self-organization in mobile ad-hoc networks: the approach of terminodes, IEEE Communications Magazine (June) (2001) 166–173.

[7] L. Zhou, Z.J. Haas, Securing ad hoc networks, IEEE Network Magazine (1999).

[8] P. Kyasanur, N. Vaidya, Detection and handling of MAC layer misbehaviour in wireless networks, in: International Conference on Dependable Systems and Networks (DSN'03), San Francisco, CA, June 2003, pp. 173–182.

[9] S. Bo, W. Kui, U.W. Pooch, Towards adaptive intrusion detection in mobile ad hoc networks, in: IEEE Global Telecommunications Conference (GLOBECOM), vol. 6, 29 November–3 December 2004, pp. 3551–3555.

[10] X. Yan, L. Ren-Fa, L. Ken-Li, Intrusion detection using mobile agent in ad-hoc networks, in: Proceedings of Inter- national Conference on Machine Learning and Cybernetics, vol. 6, 26–29 August 2004, pp. 3383–3388.

[11] Y. Zhang, W. Lee, Intrusion detection in wireless ad-hoc networks, in: Proceedings of the 6th Annual International conference on Mobile Computing and Networking, Boston, MA, USA, 2000, pp. 275–283.

[12] W. Zhang, R. Rao, G. Cao, G. Kesidis, Secure routing in ad hoc networks and a related intrusion detection problem, in: IEEE Military Communications Conference (MILCOM), vol. 2, 13–16 October 2003, pp. 735–740.

[13] Kyasanur P, Vaidya N. Detection and handling of MAC layer misbehaviour in wireless networks. In: International conference on dependable systems and networks (DSN'03). San Francisco, California; 2003.

[14] Bhargava S, Agrawal DP. Security enhancements in AODV protocol for wireless ad hoc networks. In: Vehicular technology conference, 2001, vol. 4; 2001. p. 2143–7.

[15] Borisov N, Goldberg I, Wagner D. Intercepting mobile communications: the insecurity of 802.11. In: ACM MOBICON; 2001.

[16] Dahill B, Sanzgiri K, Levine BN, Shields C, Belding-Royer EM. A secure routing protocol for ad hoc networks. In: IEEE ICNP; 2002.

[17] Hu Y, Perrig A, Johnson D. Ariadne: a secure on-demand routing protocol for ad hoc networks. In: ACM WiSe; 2002a.

[18] Hu Y, Johnson D, Perrig A. Sead: secure efficient distance vector routing for mobile wireless ad hoc networks. In: IEEE WMCSA; 2002c.

[19] Hubaux J, Buttya ´n L, Capkun S. The quest for security in mobile ad hoc networks. In: Proceedings of the second ACM international symposium on mobile ad hoc networking and computing. USA; 2001.

[20] Kaufman C, Perlman R, Speciner M. Network security: private communication in a public world. Prentice-Hall, Inc.; 1995.

[21] Marti S, Giuli TJ, Lai K, Baker M. Mitigating routing misbehaviour in mobile ad hoc networks. In: Proceedings of the sixth annual international conference on mobile computing and networking. Boston, Massachusetts, United States; 2000. p. 255–65.

[22] Menezes AJ, Vanstone SA, Van Oorschot PC. Handbook of applied cryptography. CRC Press, Inc.; 2001.

[23] Papadimitratos P, Haas ZJ. Secure routing for mobile ad hoc networks. In: SCS communication networks and distributed systems modelling and simulation conference (CNDS 2002). San Antonio; 2002.

[24] Perkins CE, Royer EM. Ad hoc on-demand distance-vector routing (AODV). IETF draft; 2001.

[25] Royer EM, Toh C-K. A review of current routing protocols for ad- hoc mobile wireless networks, IEEE Personal Communications Magazine 1999. p. 46–55.

[26] Schneier B. Secret and lies, digital security in a networked world. Wiley; 2000.

[27] Stallings W. Cryptography and network security: principles and practice. 2nd ed. Prentice-Hall, Inc.; 1998.

[28] Zhang Y, Lee W. Intrusion detection in wireless ad-hoc networks. In: Proceedings of the sixth annual international conference on mobile computing and networking. Boston, Massachusetts, United States; 2000. p. 275–83.

[29] Zhou L, Haas ZJ. Securing ad hoc networks. IEEE Network Maga- zine 1999.

[30] Q. Xue, J. Sun, Z. Wei, TJIDS: an intrusion detection architecture for distributed network, in: IEEE Canadian Conference on Electrical and Computer Engineering (CCECE), vol. 2, 4–7 May 2003, pp. 709–712.