Exploring Cross-layer techniques for Security: Challenges and Opportunities in Wireless Networks

Geethapriya Thamilarasu and Ramalingam Sridhar
University at Buffalo, Buffalo, NY 14260-2000
{gt7, rsridhar}@cse.buffalo.edu

Abstract—In this paper, we discuss the challenges and opportunities of using cross-layer techniques for enhancing wireless network security. Cross-layer approach has gained considerable interest in performance optimization due to their design advantages. While the architectural modification introduced by the inter-layer interactions show promising results on overall network performance, there is also a growing concern on their limitations. Here, we investigate the impact of cross-layer techniques on security and network performance. An in depth understanding of the strength and weakness of cross-layer methods is necessary in designing robust architectures. To this end, we evaluate different cross-layer architectures and analyze their efficiency in intrusion detection systems.

I. INTRODUCTION

With the rapid growth and development of wireless networks, determining an appropriate architecture for the wireless network protocol stack remains an open challenge. Though layered communication paradigm has been successful in traditional wired networks, such as Internet, it poses several limitations in wireless networks. For instance, in wireless networks, the channel error at lower layers is often mistaken as congestion at the network layer resulting in poor TCP throughput [1]. Due to the varying channel conditions and dynamic network topology of wireless networks, it is important for the layers to coordinate and adapt to the environmental changes. Adopting a strictly layered approach in wireless domain places constraints on network interoperability, flexibility and adaptivity. Co-operation between the layers is thus necessary to reach higher adaptivity and optimal network performance. Also, more often in wireless networks, there is a requirement for autonomous network operation with minimum human intervention. Design of such self-dependent and decentralized systems requires modifications to existing architectural designs. Recent research efforts indicate that cross-layer design architectures can efficiently address these challenges in wireless networks.

Cross-layer designs typically combine or extract information from two or more layers of the protocol stack. Information is shared either between adjacent layers or non-adjacent layers to create a system with an ease of adaptability. By interfacing and interacting between the protocol modules in different layers, we can create wireless architectures with better holistic views of network goals and constraints. Although several cross-layer techniques are currently explored for enhancing network performance, there is limited work on applying them in the context of wireless security. Our main contribution in this paper is to investigate the suitability of cross-layer architectures in intrusion detection systems. We also explore the various cross-layer design restrictions and study their feasibility in order to build efficient and reliable intrusion detection systems.

II. CROSS-LAYER DESIGN IN WIRELESS NETWORKS

Varying definitions and classifications of cross-layer design can be found in the recent literature. Srivastava et al [2], define cross-layer as a simple violation of a layered communication architecture. Such violations may occur in different ways, either by merging adjacent layers, or by creating new interfaces between adjacent layers or through a shared database between the layers. Yuan et al [3] propose a cross-layer adaptation GRACE to conserve energy and improve QoS in mobile multimedia terminals. GRACE is an adaptation framework that performs only local adaptation by interfacing system layers to a central resource manager that acts as a coordinator. The manager mediates between the layers to obtain a proper combination of configurations for each layer to achieve optimal results.

In [4], ECLAIR- a two tier architecture consisting of Optimization SubSystem (OSS) and Tuning Layers (TL) is proposed. In this architecture, optimization algorithms are incorporated into the framework of OSS cross-layer engine. TL provides user feedback such that the protocol stack is modified according to user priorities. In [5], Cross-layer approach to self-healing (CATS) was proposed for sensor networks and battlefield applications.

1-4244-1513-06/07 $25.00 ©2007 IEEE
CATS introduces a new component called the Management plane which is visible across all layers. This plane provides all the self-healing functions and influences protocol behavior such as altering changes to a routing protocol. The disadvantage of this framework however, is introducing new protocols and applications, also results in a change in the underlying framework itself.

MobileMan [6] is another design that identifies security, energy management and cooperation as general objectives that are cross-layer in nature. This architecture has a central component called the network status that stores information about all protocols in the network. The network status acts as an indirect interface between the layers. The problem with this architecture however is that it limits the amount of possible protocols running inside the framework. WIDENS-Wireless DEployable Network System is a cross-layer project proposed for public safety, emergency and disaster applications [7]. These cross-layer extensions assume a centralized server, provide for protocol state interactions and parameter mapping between the layers.

From the perspective of enhancing network performance, researchers are currently exploring several cross-layer interactions. However there is limited work in exploring the cross-layer design in the realms of network security. Zhang et al [8] proposed the idea of a multi-layer intrusion detection for wireless ad hoc networks using a statistical anomaly based detection model. In our previous work, we have demonstrated a cross-layer based intrusion defense architecture [9]. We have also analyzed the specific case of detecting Jamming attacks in wireless networks using cross-layer techniques [10]. From our earlier work, we have observed that adopting cross-layer designs for security yields efficient performance improvement. However, it is also important to study both their benefits and limitations in order to provide a standardized intrusion detection module for wireless networks.

A. Exploring the Limitations

Cross-layer methodologies are prone to certain restrictions and limitations according to the nature of their designs. It is possible that providing interfaces between the layers might sometimes lead to conflicting results on the network performance. Detailed investigation of these challenges will provide an insight into the development of more efficient and reliable cross-layer adaptation mechanisms. Kawadisa et al [11] provide a detailed analysis of cross-layer design principles and emphasize the need to exercise strong caution while proposing such architectural changes. In this section, we examine these limitations involved in adopting cross-layer design techniques.

1) Loss of Modularity: The success of Internet today is primarily attributed to its OSI protocol stack architecture. This layered architecture provides the abstraction and modularity to independently design protocols. With cross-layer interactions however, the layering structure is broken and the network design becomes complicated. Researchers lose the flexibility and capability of designing a particular protocol layer without impacting other layers.

2) Interactions and Unintended Consequences: Cross-layer couplings enable information sharing and assist in network optimization. Creation of such interdependencies across protocol layers may inadvertently cause performance losses. For instance, an implementation change to the MAC protocol at the lower layer may affect the performance of a routing protocol at the network layer, by creating paths with longer hops and delays. It is hence important for the designers to account for these layer interactions.

3) Adaptation loops: Another significant challenge with information transfer between higher and lower layers is the potential creation of adaptation loops in the system. When an uncontrolled interaction occurs, each layer may become dependent on information from another layer leading to loops and causing system instability.

4) Chaos of Unbridled Cross-layer designs: Since there are no independent layer modules in a cross-layer architecture, their implementation using network tools is a big challenge. Designers fear a software implementation of the cross-layer design might result in an unstructured spaghetti like code [11].

Addressing the limitations after designing a system in its post deployment stage will not be very effective. It is thus necessary to account for these shortcomings while developing the architecture framework. Proper handling of the design inadequacies and exploitation of benefits will lead to robust cross-layer architectures.

III. CROSS-LAYER OPTIMIZATION IN WIRELESS SECURITY

Literature reveals that cross-layer design leads to performance optimization in terms of bandwidth, energy and other resources. Although cross-layer techniques have been discussed in the recent past, their effects on securing the wireless network and assisting in intrusion detection is yet to be explored in depth. In this section,
we discuss the possible benefits involved in incorporating cross-layer methods in an intrusion detection system.

A. Motivation for Cross-layer in Security

Security is an important concern in wireless networks due to their increased vulnerability and exposure to varying types of attacks. Unreliable wireless links, constantly changing network topology and lack of a centralized system to handle the security needs of the network contribute to insecure standalone systems in wireless networks. Intrusion detection systems located on concentrated points such as network gateways and wireless access points are not guaranteed to achieve the desired security level in the network. This explains the need for an efficient intrusion detection system to manage the access control and provide a monitoring unit to observe any abnormal behavior in the network.

In a wireless network protocol stack, every layer is vulnerable to attacks (internal and external) by adverse nodes in the network. Independent security solutions at different layers might lead to conflicting actions and result in performance degradation. Hence, ensuring security and network reliability, has to be jointly addressed in all of the protocol layers. Proper interaction and coordination among different protocol layers helps in developing a robust intrusion detection system suitable for wireless networks. Such interactions are the key elements to building cross-layer architectures.

Apart from the need to make a collaborative decision, adopting a cross-layer approach to intrusion detection facilitates effective fault diagnosis and reduced false alarms. Most often, the intrusion detection systems fail to distinguish malicious activity from faulty network behavior that may occur due to non malicious reasons. Higher false positives is a significant problem in current intrusion detection systems. This is primarily because existing IDS are not reactive to the changes in the network. They do not utilize current network or system information available from other layers toward making their decision. Interacting with other layers and accessing vital channel and network information to judge the malicious nature of a node lowers the false positives to a great extent and assists in an efficient detection diagnosis.

IV. CROSS-LAYER ARCHITECTURE FRAMEWORK FOR INTRUSION DETECTION

In the previous section, we emphasized the importance and need for adopting cross-layer interactions in wireless network security. However, certain limitations of these designs, may sometimes present themselves as an impediment to the development of successful architectures. It is evident that standardized cross-layer adaptation mechanisms are required that can overcome their inherent challenges and enhance network performance.

Although there is no standard architecture, cross-layer couplings or combinations mostly occur through direct interaction between the layers or through a structured method using a shared database [2]. In this work, we investigate these two cross-layer architectures to assess their efficiency in optimizing network security.

A. Cross-layer IDS based on Direct Per-layer Interactions (Type I)

We have developed a Type I intrusion detection system for improved detection and better evaluation of malicious activity in the network. In this type of cross-layer architecture, information is exchanged directly between two adjacent or non-adjacent layers of the protocol stack, such that, the layer adaptations result in improved end-to-end network performance. Figure 1 gives a schematic overview of the IDS module.

In this design, every layer in the network protocol stack collects audit data by actively monitoring the channel. When an anomaly is detected in a particular layer using its audit data information, it triggers or initiates detection at another layer. Such probe based or event based detection helps in confirming the malicious behavior of a node. For instance, malicious packet drop in a network can be observed and detected through promiscuous network monitoring watchdog schemes. However, in wireless networks, packet drops can also occur due to poor channel quality, link contention or network congestion. Hence, apart from relying on the network statistics from an individual layer, we can confirm the presence of this attack using the knowledge of current channel conditions from the lower layers.

![Type I- Direct Layer Interaction Model](image-url)
Through such direct exchange of information between layers, IDS can detect intrusions with a higher confidence level. Simulation results from our earlier work, as shown in fig.2 and fig.3 demonstrate this scenario and illustrate the effectiveness of such IDS in improving the accuracy of detection while also lowering the false positives [9]. Although cross-layer based IDS presents promising results in terms of detection efficiency, there are certain shortcomings associated with these designs in terms of overall system optimizations. In the following, we elaborate the architectural limitations of this design.

1) Influences of Detection Protocol: Direct interactions between the protocol layers in a cross-layer system might sometimes result in unintended network consequences. For instance, in our previous example, if the congestion information is used by the detection protocol in other layers to confirm malicious behavior, it leads to improved detection as shown by the results. But, if there exists another cross-layer network optimization design that chooses network routes according to the congested state of the network, then the exchange of detection information might lead to adverse routing protocol consequences.

The information passed on to the network layer might influence the routing protocols to choose less congested paths. Such paths may either consist of longer hops or higher percentage of malicious nodes and thus negatively impact the overall network performance. Figure 4 shows that the plain scheme without a cross-layer detection actually has a higher network throughput compared to detection using cross-layer system with direct layer sharing. Coexistence of various cross-layer optimizations is still an ongoing research.

2) Internal Overhead: Since the local detection mechanisms do not involve communication within a network, they do not incur any external overhead. However, the communication between the layers through internal packets results in internal overhead in a node. The size of the overhead is proportional to the size of the audit data information collected through the internal packets. Availability of more information to share amongst the layers means efficient IDS with fewer detection errors but with high internal overhead. Thus there exists a trade-off between obtaining lower false alarms at the cost of internal overhead.

3) Stability: Another weakness with this type of cross-layer design is that it might result in system instability. Since detection information may be relayed back and forth between the layers, it may cause adaptation loops in the system. Care should be taken to avoid such loops while adopting cross-layer based schemes. Time scale separation principle is considered as a solution to address system instability [11]. In our case, we can control triggering the detection for intrusions by allowing controlled and atomic access to the parameter under different timescales. In order to make our design failsafe and more robust, we provide an on-demand notification scheme where intrusion detection is triggered at other layers only when probed by higher or lower layers. For instance, when a threat is detected at the network layer, the intrusion detection system probes for any further information on the network conditions or security threats from another layer by sending a probe request to the corresponding layer(s). Obtaining this additional information supplements the detection mechanism.

4) Modularity: Another disadvantage of detection using direct cross-layer designs is the loss of modularity in the protocol stack. Since detection approaches at different layers are no longer functionally independent, they impact each other and significantly affect the network optimizations. It is important to account for these architectural design weakness to develop a robust IDS in wireless networks. Through suitable modifications and enhancements to the framework and addressing the above limitations of cross-layer based designs, we can build a stronger and successful intrusion detection architecture for wireless networks.
TABLE I
COMPARISON OF CROSS-LAYER ARCHITECTURES

<table>
<thead>
<tr>
<th></th>
<th>Type I</th>
<th>Type II</th>
<th>Non Cross-layer</th>
</tr>
</thead>
<tbody>
<tr>
<td>Detection Efficiency</td>
<td>HIGH</td>
<td>HIGH</td>
<td>LOW</td>
</tr>
<tr>
<td>DR</td>
<td>VERY LOW</td>
<td>LOW</td>
<td>HIGH</td>
</tr>
<tr>
<td>Modularity</td>
<td>LOW</td>
<td>MEDIUM</td>
<td>HIGH</td>
</tr>
<tr>
<td>Stability</td>
<td>LOW</td>
<td>MEDIUM</td>
<td>HIGH</td>
</tr>
<tr>
<td>Protocol Complexity</td>
<td>HIGH</td>
<td>LOW</td>
<td>-</td>
</tr>
<tr>
<td>Implementation Complexity</td>
<td>HIGH</td>
<td>LOW</td>
<td>-</td>
</tr>
<tr>
<td>Resource Consumption</td>
<td>LOW</td>
<td>HIGH</td>
<td>-</td>
</tr>
</tbody>
</table>

It is simpler and easier to manage this type of detection system due to separation between the protocol layers. The database unit possesses a local and global view of the network. An intelligent optimizing unit in the detection system ensures that the detection scheme can react and adapt according to the varying threat level in the network. This type of architecture is in general preferred to direct layer interactions due to the following reasons:

1) Modularity: In the structural design of shared IDS, protocol interactions occur through a well defined interface to a common database system. This ensures that the modularity of the network protocol stack is preserved to a certain extent. Instead of exposing the information across all layers, only the minimum necessary information is shared. Interface to the database thus enables parallel and independent evolution of the layers. As the protocol influences among the layers are kept at a minimum, it improves the system efficiency.

2) Stability: Since the layers of the protocol stack do not communicate directly with each other, and each layer interacts with a shared database, the system facilitates a controlled information transfer. As the database is responsible for coordinating detection information gathered across the layers, there is minimum possibility of loops created among the layers. This adds stability to the network.

3) Implementation Complexity: This model has significant overhead in terms of updating parameter information obtained from all layers. However, when compared with Type I architecture, it has a lower cost of implementation. This is because every layer in Type I performs monitoring and triggering the network for intrusions. Type II scheme on the other hand, obtains the state information from the layers and triggers detection on a need basis.

Table I gives a sketch of the differences between the two cross-layer architectures. While both the architectures seemingly perform well in terms of improving the detection accuracy, there are significant differences...
in overall system optimization. Thus, based on the requirements, we must choose the appropriate design for intrusion detection system.

V. OPEN CHALLENGES AND FUTURE DIRECTIONS

Research on various cross-layer techniques and methodologies is still in its incipient stages. Some of the open challenges associated with cross-layer designs are:

- Can a cross-layer framework designed for optimizing network security be coupled with other cross-layer based network optimizations?
- Can we standardize an intrusion detection framework for wireless networks based on the proposed cross-layer architectures?
- Can we have the choice and flexibility to invoke different cross-layer designs based on the threat or security level in the network?
- How to evaluate the fundamental trade-offs between the network performance and security architecture?
- How to determine a common platform to implement cross-layer design proposals and study their performances using simulations?

Although there is no definitive answer, lack of interoperability between various cross-layer optimization goals is one of the main problems with various current solutions. To build an efficient network, it is essential to optimize different goals simultaneously. Joint optimizations will provide reliable networks, however, this might complicate the network design to a great extent.

Developing a standardized detection framework for wireless networks, will improve the accuracy of detecting malicious intrusions. For this, we must first explore the possibility of adopting different cross-layer architecture. In this paper, we have provided a performance comparison between two cross-layer detection systems. From our results, we can standardize the shared database model for detecting intrusions. However, if there are other choices, we should also consider them.

Future research work in cross-layer designs, must focus on solving the above mentioned challenges. This will determine the success of cross-layer architectures in wireless networks.

VI. CONCLUSION

In this paper, we discussed the cross-layer architectures and examined their benefits and limitations in detail. In particular, we investigated the impact of cross-layer designs in optimizing network security. We evaluated an intrusion detection framework using two different types of cross-layer architectures based on direct communication between layers and using a shared database model. We observed that while both the designs yielded higher detection accuracy, the shared database model performed better in terms of higher system stability and lower implementation complexity. Through careful consideration of the shortcomings and proper exploitation of cross-layer techniques, we can thus build robust intrusion detection systems for wireless networks.

REFERENCES