Enhanced Anomaly Intrusion Detection System for Mobile Ad Hoc Networks

Kosmas Kapis
Department of Computer Science and Engineering – College of Information and Communication Technologies
University of Dar es Salaam, UDSM
Dar es Salaam, Tanzania
E-mail: kapis [AT] udsm.ac.tz

Samwel Magesa Bairi
Department of Computer Science and Engineering – College of Information and Communication Technologies
University of Dar es Salaam, UDSM
Dar es Salaam, Tanzania

Abstract—**The rapid proliferation of wireless networks and mobile computing applications has changed the landscape of network security. The wireless Ad Hoc network is particularly vulnerable due to its features of open medium, dynamic changing topology, cooperative algorithms, lack of centralized monitoring and management point, and lack of a clear line of defense. Many intrusion detection techniques have been developed but have a high memory usage. New architecture and mechanisms to decrease memory usage in wireless networks and mobile computing application have to be developed.**

This paper proposes an enhanced mechanism in which IDS for mobile devices can decrease memory usage and improve response time thus increasing life span of Ad Hoc devices. The proposed solution is achieved by studying AES and TEA algorithms, then come up with the most effective solution. The prototype is built by combining both separately AES and TEA algorithms and path.

Keywords-Security, Integrity, Detection, Encryption, Mobile Networks, Ad Hoc, Intrusion, Power Conservation

I. INTRODUCTION

This field of research is called Intrusion Detection. The possibilities and opportunities in this field are limitless, unfortunately, so too are the risks and chances of malicious intrusions. It is very important that the security mechanisms of a Mobile Ad Hoc Network (MANET) system are designed to prevent unauthorized access to system resources and data. However, completely preventing breaches of security appear, at present, unrealistic. Efforts have been made however to detect these intrusion attempts so that action may be taken to repair the damage later. This field of research is called Intrusion Detection.

Intrusion Detection can be used in A Mobile Ad Hoc Network (MANET), which is a collection of wireless nodes that can dynamically form a network to exchange information without using any pre-existing fixed network infrastructure. Such a network requires a field of pervasive environment. This facilitates the communication between the mobile devices. Attractive applications of MANET include Military battlefield, commercial sector, Personal Area Network (PAN). That would mean forming a temporary network with devices with mobility and local level.

Regardless of the attractive features of MANET, it still faces several challenges. Security is one of the vital issues in MANET. Since Ad Hoc network rely on wireless communication medium, it is important to provide robust ways of detecting attacks before they affect the network. Mobile Ad Hoc network applications are increasing due to the tremendous growth of personal devices and ubiquitous techniques. Hence, the number of users of a network may increase and consequently the number of attacks may increase. For minimizing this practical weakness, strong Intrusion Detection System (IDS) are needed to capture real attacks with higher accuracy [1]. This will fill the network security gap that has drastically emerged due to the rapid increase of wireless devices, networks and applications. New vulnerabilities are created due to mobility which is not present in a fixed wired network, and so many of the proven security measures turn out to be ineffective.

Due to ineffectiveness of firewalls a second line of defense of IDS is highly needed to secure Ad Hoc devices, as shown in Figure 1. According to [2], an IDS is used to detect all types of malicious network traffic and computer usage that cannot be detected by a conventional firewall. In addition, IDS is able to resist external attacks. One of the major problems with current IDS is that they consume too much memory [3] or with increase size of the network [4].

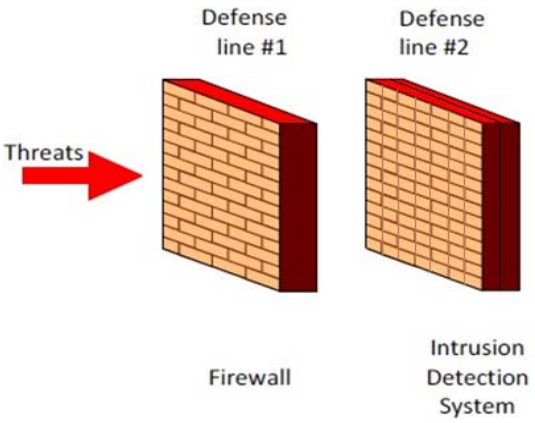

Figure 1: Security Defense Lines

The current memory consumption of current IDS is too high hence limiting the capabilities of the IDS. When the IDS consume too much memory it becomes less effective in detecting the intrusion hence increasing the number of false alarms. But also another limiting factor discussed in this research is the response time for the IDS. The higher memory usage increases the power utilization in Ad Hoc devices.

In addition [5], indicated that Ad Hoc systems become a single point of failure if the deployed IDS system is disabled for any reason, then it often give an attacker the time to compromise the system and possibly gain a foothold in the network.

The study uses anomaly-based approach to find for behavior of computer resources deviating from normal behavior. The underlying principle of this approach is that "attack behavior" differs enough from "normal user behavior" thus it can be detected by cataloging and identifying the differences involved. First, the "normal" behavior must be well defined, which is not an easy task. Once normal behavior is fully qualified, irregular behavior will be tagged as intrusive. Therefore IDS analyze information from a computer or a network to detect malicious actions and behaviors that can compromise the security of a computer system. When a malicious behavior is detected, an alarm is launched.

This study aimed at improving detection for MANET as described in other studies, working of procedure for minimizing memory usage, discovering further information security challenges faced also proposing suitable alternatives to address those challenges and in turn a prototype for new requirements showing feasibility of the proposed solution.

II. METHODOLOGY

Lucienne and Amaresh in [6] and Lacey and Luff in [7] suggested that a methodology that can be used for development of the prototype has to follow the certain pattern which in this case was to derive the functionalities of the prototype from the prototyping process itself.

A. The Approach

The approach that was used is entirely based on anomaly based method, which has been used to address security problems related to attacks in a wireless networks. This research however extended the anomaly method by separating the intrusion detector into functional layers. That is each layer in the hierarchy will be responsible for a specific functional task in the IDS based on the algorithms that have been configured for that specific layer.

B. Prototype Architecture

Similar to this model, the Layered IDS represents a sequential Integrated Layered Approach and is based on ensuring availability, confidentiality, and integrity of data and services over a network. The goal of using a layered model is to reduce computation and the overall time required to detect anomalous events. The time required to detect an intrusive event is significant and can be reduced by eliminating the communication overhead among different layers. This can be achieved by making the layers autonomous and self-sufficient to block an attack without the need of a central decision-maker.

The prototype architecture defines how the prototype is built and basically how do parts of the prototype relate to one another. It defines the relation between the parts of the prototype as well as explaining how each part of the prototype is very essential in accomplishing the functionalities of the other parts. Since the prototype aims at proving that, the enhanced prototype design which for Ad Hoc networks has a higher response time and lower memory usage, the architecture of the prototype will have to incorporate all the essential parts of the intrusion detection system. The architecture will also have to incorporate the parts of path security. Good prototype architecture provides a road map for the prototype building process, by putting the prototype components into perspective, defining the functionalities of the prototype components, and demonstrating how they interact with one another.

C. Prototype Implementation

After all of the requirement were gathered, the prototype design was put into place. The prototype was implemented. Building the prototype had to account for a lot of factors as how the prototype will be tested and how will it run to deliver the best results that is intended from the research. The prototype was developed using Java codes.

Since several detection algorithms that already exist for detecting malicious activities. The main activity of this subsection however was not to develop a new algorithm, rather using the best out the existing algorithms to create a combination of algorithm and detection engine that can be

used to express the logic of multilayer intrusion detection and achieve minimal memory usage and maximum response time.

The algorithm of AES and detection that have been chosen for the implementation after they were translated to java code from the pseudo code, the logics were then applied into the built program.. Logics were the conditions that will have to be followed to detect the malicious intrusions. It is like a body of rules that will define what is malicious and what is not, the logic in java will also define the recommended action that the system should take when encountering such cases. AES was chosen since it uses simple encryption techniques as compared to TEA

A file with malicious codes which contains harmful intrusion is sent from one machine to another and the prototype is tested if it performs to the required expectation.

D. Algorithm

Figure 2 shows the detailed cycle of the whole algorithm. First is the path security which breaks the message into 40 byte strings, thus terming the not 40 byte messages as intrusions. Also the algorithm encrypts/decrypt messages as seen from the flow of event.

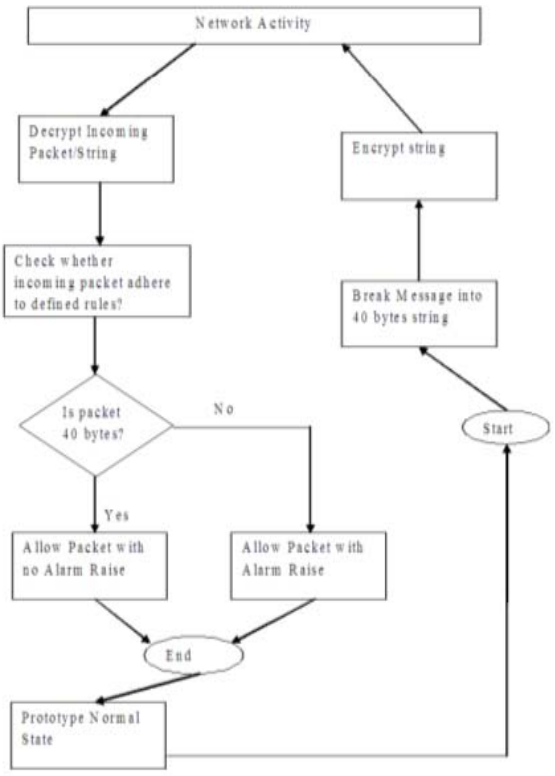

Figure 2: Algorithm

III. RESULTS

The following are the samples of different scenarios taken which show the performance of both AES and TEA in parameter settings which differ.

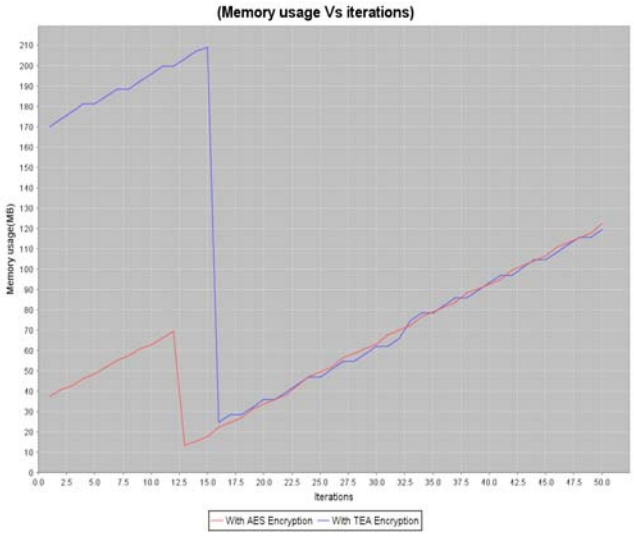

Figure 3: Memory Usage

In the first part of sample 1 as shown in Figure 3 the average memory usage of AES was recorded to be 70MB while that of TEA was recorded at 115MB. The iteration chosen of 2.5cycle/sec, 25 cycle/sec and 50 cycle/sec were chosen specifically representing the overall graphically structure, 2.5 is the first point of the x-axis, 25 is the centre of the graph, and 50 is the last point of the x axis.

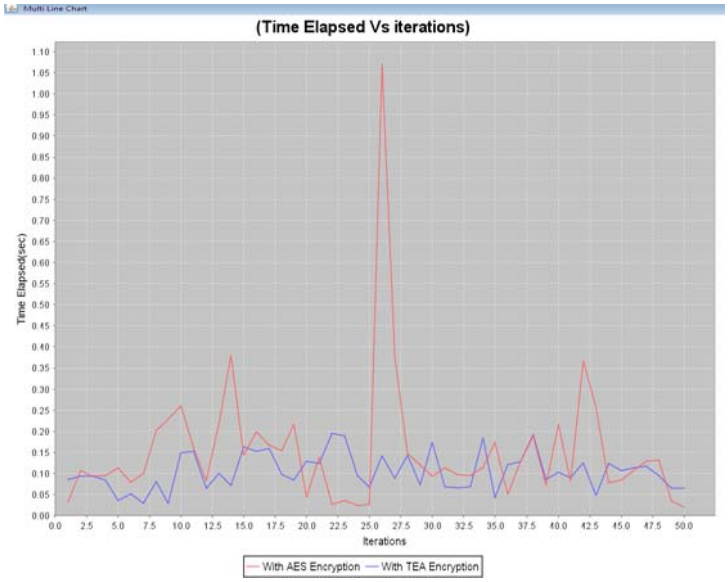

Figure 2: Response Time

In the second part of sample 1 as shown in Figure 4 the average memory usage of AES was recorded to be 0.05Sec while that of TEA was recorded at 0.08Sec. The iteration chosen of 2.5 cycle/sec, 25 cycle/sec and 50 cycle/sec were chosen specifically representing the overall graphical structure, 2.5 is the first point of the x-axis, 25 is the center of the graph, and 50 is the last point of the x axis.

E. Sum of Memory Usage and Response Time

Figure 5 shows the summation of all the memory usage values from the earlier identified samples. These are accumulative figure for memory usage both AES and TEA summed separately as follows 75.38MB (AES) and 120.49MB (TEA).

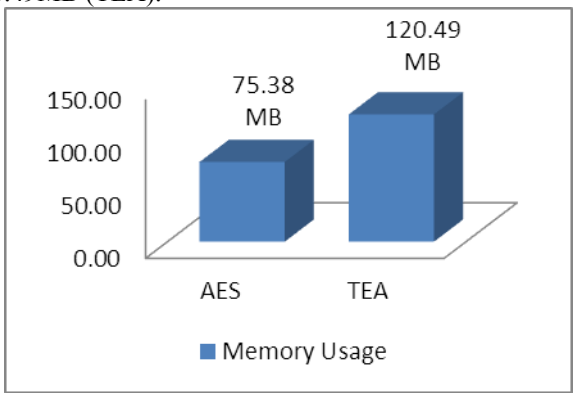

Figure 3: Total Memory Usage

Figure 6 however shows the summation of all the response time values from the earlier identified samples. These are accumulative figures for response time both AES and TEA summed separately as follows 55.73Sec (AES) and 52.48Sec (TEA).

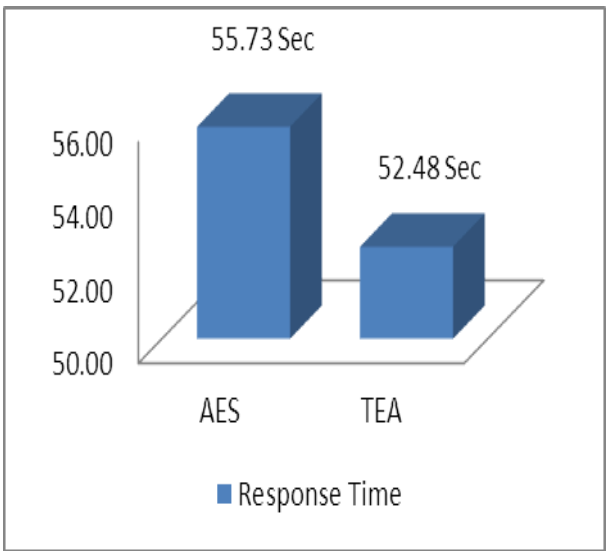

Figure 4: Total Response Time

F. Average of Memory Usage and Response Time

From the calculated sum in Figure 6 the average was found by simply dividing the total figure derived by the number of samples that were used in testing and evaluation. The number derived was then recorded as follows 12.56MB (AES) and 20.08MB (TEA) and was used to draw the bar chart in Figure 7 and the pie chart in Figure 8.

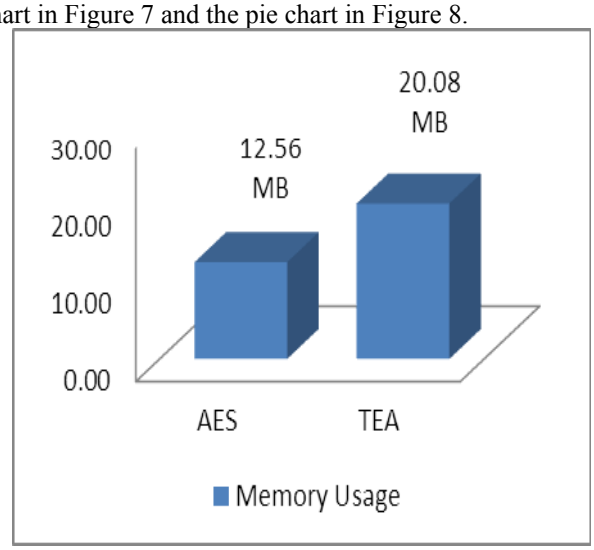

Figure 5: Average Memory Usage

The pie chart of Figure 8 was drawn from the values obtained from 12.56MB (AES) and 20.08MB (TEA).

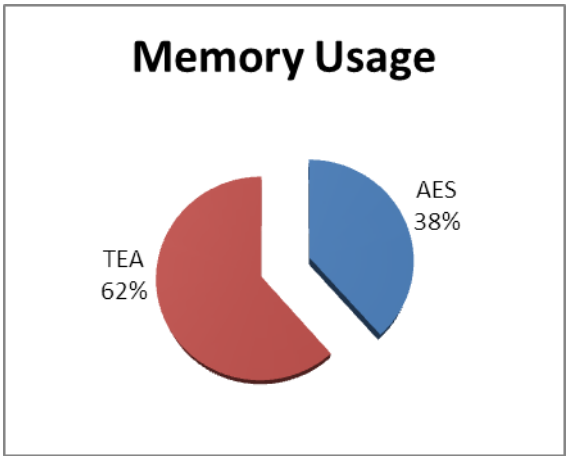

Figure 6: Average Memory Usage

From the calculated sum in Figure 7 the average was found by simply dividing the total figure derived by the number of samples that were used in testing and evaluation. The number derived was then recorded as follows 9.29Sec (AES) and 8.75Sec (TEA) which was used to draw the bar chart in Figure 9 and the pie chart in Figure 10. The bar chart of Figure 9 was drawn from the values 9.29Sec (AES) and 8.75Sec (TEA).

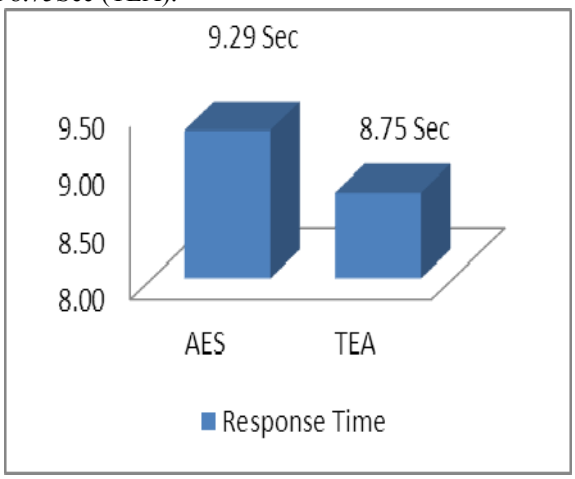

Figure 7: Average Response Time

The pie chart of Figure 10 was drawn from the values obtained from values 9.29Sec (AES) and 8.75Sec (TEA).

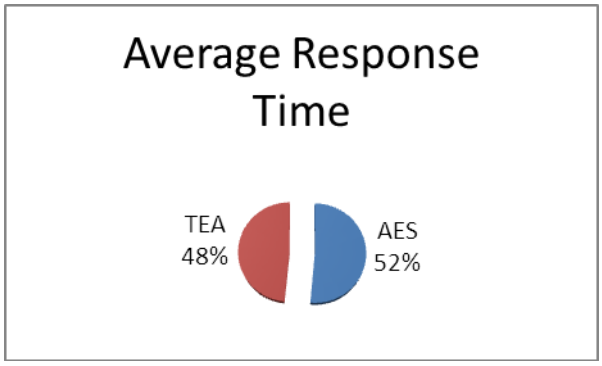

Figure 8: Average Response Time

From analysis of the provided Tables, Charts and Figures AES encryption seemed to perform much more efficient as compared to TEA encryption as far as the analysis is concerned. Referring to the Figure 7, AES has an average memory usage of 12.56MB, while TEA encryption has an average memory usage of 20.08MB. Meaning that there is a difference of 7.52MB usage between AES and TEA encryption of the developed IDS on average. This is a significant amount of memory that could be used for other processes thus increasing the IDS capabilities as well as improving its life time.

This further implies that, on average AES encryption will use less memory when used for security purposes. On the other hand from Figure 9 AES encryption has response time 9.29Sec while TEA encryption has a response time of 8.75Sec. The response time simply means the time it takes for IDS to detect the intrusion and issue the appropriate response. These response times are measured when the IDS are used with the two different encryption used in this research. There is a decreased differenceof 0.54Sec.

IV. DISCUSSION

This paper has attempted to propose a system solution to a enhance anomaly intrusion detection for Mobile Ad Hoc Networks. This has been effected by firstly, effectively conducting threat analysis using attacker centric model. The attacker centric model allows effective identification of common threats. This was important in understanding the overall performance bottleneck of high memory usage in IDS. Secondly, a prototype has been built from a developed algorihm using java programming language. It has been built by defining the packet size for transmission and type of encryption defined in the algorithm. Finally, the newly developed memory usage minimization algorithm has been enforced.

The memory usage minimization algorithm detects the intrusion based on packet structure as well as secures the

channel through which data is transmitted. The algorithm has demonstrated to be very effective in reducing memory usage. It is recommended for further refinery in the future IDS development. Results in the work presented in this paper shows that memory usage was minimized by 24% as depicted in Figure 7.

V. FUTURE WORK

The research encountered some few setbacks like slow response of the respondents and access to some of the vital information that was needed in data collection process. It also encountered some few difficulties in refining the prototype of the previous research in the current research environment so that the results can be compared from the similar platform.

A combination of procedures and algorithms with a selected encryption technique that will enable an IDS to be faster, use less memory, have a highly response time is required. Figures attained in this research can further be improved through different techniques or the combination of them.

The study recommends a fine tuning between the rules of defining intrusions and securing the medium and form in which the data is communicated has to be highly prioritized to be sought. This clear fine tuning of the two could result in the creating light IDS hence significantly affecting response time.

REFERENCES

[1] Kumari, H. J. (2012). A hybrid Certificate management for mobile ad-hoc networks. IJCSNS International Journal of Computer Science and Network Security, pp. 112-136.oc. London, vol. A247, pp. 529–551, April 1955. (references)

[2] Mohammadreza, E. (2010). Intrusion detection using data mining techniques. International Conference on Information Retrievel and knowledge management (CAMP) , pp. 200-203.

[3] Lee, W. (2001). A data mining Framework for construction features and models for intrusion. Columbia University: Columbia.

[4] Razaque, A. and Khali, E. (2012). Fostering privacy of users in mobile collaborative. ASEE Northeast Section Conference, pp.562-578.

[5] Shon, T. (2006). Applying genetic Algorithm for classifying anomalous TCP/IP packets. Journal of Neuro computing , pp. 24292433.

[6] lLucienne, B. and Amaresh, C. (2008). Design research methodology. Springer: London.

[7] Lacey, A. and Luff, D. (2001). Trend Focus for research and development in primary health care, An introduction to qualitative analysis. Springer: London.