Elysium Journal of Engineering Research & Management

P-ISSN: 2347-4408
E-ISSN: 2347-4734

SURVEY ON NETWORK DEFENCE SYSTEM [NDS] FOR CRYPTOGRAPHY AND HYBRID NETWORK SECURITY SYSTEM

S.Venkateshbabu[1], R.Kartheeswaran[2]

[1]*Associate Professor, Department of Computer Science and Engineering, Christian College of Engineering and Technology, Dindigul, Tamil Nadu -624619 India. Email: Venkateshflower6@gmail.com*

[2]*PG Scholar, Department of Computer Science and Engineering, Christian College of Engineering and Technology, Dindigul, Tamil Nadu -624619 India. Email: annaikarthees@gmail.com*

Abstract: ***Many computing systems have recently and preventing hacking is important in protecting business. Many significant security methodologies have been proposed to provide security between hacking. Fortunately, hacking attempts can be minimized if the pre-hacking step is executed; the process is scanning, which investigate and good counter measures are in place. The scanning process provides the hackers with necessary information about the hacked systems which forms their hacking strategies. Therefore, in this paper we proposes a security solution which makes scanning process harder by addressing the properties, that makes hacking strategies against protected computer networks tedious. Our security methodologies protects the networks by generating a distinct protocol dynamically to replace the standard protocols and network paths periodically in order to puzzle the scanning attempts, and hacking the network.***

Keywords: Mobile Ad hoc Network, Cryptography, Network security, hacking.

1. INTODUCTION

The mobile ad hoc network is a new model of self-configuring, infrastructure less, wireless communication and has gained increasing attention from networking environment, mobile ad-hoc networks have to deal with many hacking threats. Since devices in mobile ad hoc networks can move freely, they can change their links to other devices. In mobile ad-hoc network, dynamic network topology routing plays an important role in the networks performance. The hackers will target the weakest link in routing target of mobile ad-hoc network. Many research and studies have been attempted to deny the hacking strategies. It is difficult to propose a routing protocol which can protect the network operation in every environment. Typically a secure protocol is only good at protecting the network against one specific type of attacks.

Many secure routing protocols have been proposed to estimate the performance of mobile ad-hoc networks. The main aim of the research is to observe the additional cost added while providing the security features to the ad-hoc networks.

The additional cost includes delay in packet transmission, the low rate of data packets over the total packets sending in the edge node.

In real time, networks will not operate perfect in every situation, which means hacking attempts, threats, malicious attacks may takes place on the network which may reduce the performance of the network. We need to study the performance of routing protocol in malicious environments, which evaluate the performance of ad-hoc networks. In this paper, we implemented two secure routing protocols: a secure version of the dynamic source routing DSR ARIADNE and Secure Ad hoc On-demand Distance Vector routing protocol SAODV in the OPNET simulation environments. By implementing several attacks in the simulation environments, malicious scenarios are created.

By implementing secure routing protocols and running these two routing protocols in malicious environments. I have evaluated those secure routing protocols, and have proposed solutions. To remove the weaknesses and/or to improve the performance of these secure routing protocols DSR benefits from source routing since the intermediate nodes do not need to maintain up-to-date routing information in order to route the packets that they received.

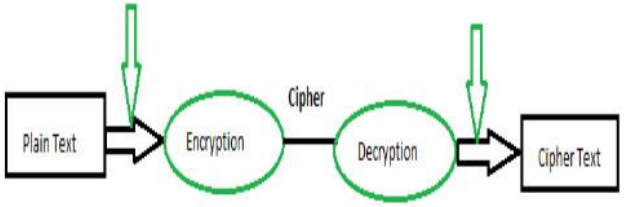
2. RELATED WORK

Network Defense System uses network to analyze, monitor, and prevent against hacking attempts degrading the network performance. The networks data packet can be secured by encrypting the data packets that are sent over the network. The networks can be protected by firewall. The best option to detect the hacking attack is to monitor the weak link nodes.

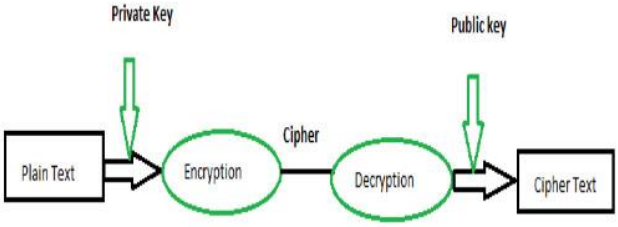
Cryptography is also knows as secret coding which hides the meaning of the data only authorized user can view the transmitted data. When an unauthorized user hack the transmitted message only non-readable message is show to that user. Converting the data into unreadable format is called the ciphering. Converting the unreadable format into human readable format with the keys is called the deciphering.

In olden days Cryptography is done using asymmetric keys system, where the sender encrypts the original message with the encryption key and the receiver decrypts message with the encryption key. Both sender and receiver have the encryption key. Meanwhile a hacker can crack the key and view the encrypted message.

P-ISSN: 2347-4408
E-ISSN: 2347-4734



In modern days symmetric keys system is implemented, where the sender and the receiver have the public key, meanwhile the receiver knows the private key which is used to decrypt the message.



Cipher texts can be accessed by hacker, but they cannot view the plain text. Hacker cracks the encryption key with the frequency of word analysis. This type of attack is called the Ceaser Cipher.

Nowadays Cryptography techniques are used in banking sectors, medical fields and in government sectors. We use various security algorithms like RSA algorithm, AES algorithm, Hash functions, digital signatures, firewalls, SSL certificates etc.

Issues in cryptography:

- Time consuming.
- The amount of cipher text is higher than the plain text.
- When key is decrypted then whole system is spoiled.

To overcome these issues:

1) We can compress the cipher text
2) Less number of key usage during encryption

In modern days the user data is compressed and then encrypted with the private key and then cipher text is compressed again and transmitted to the receiver.

At the receiver end cipher text is decrypted and decompressed to get the original data.

SYN Flooding is one of the attacks in Manet, where intruder send the huge packets without any acknowledgement, in receiver side large packet data gets accumulated and crashes the receiver node.

Smurfing is process by which hacker send the echo packet data to the receiver. When receiver sends the echo packet to other user, the end user nodes is now vulnerable to the attack. Denial of service, hacker installs custom attack script in machines and distribute attack script to large number of machines over a period of time.

The Dynamic Source Routing Protocol forms on-demand route when transmitting node requests one. In source routing, source node has the accumulating address from source to destination node addresses. The accumulated path information is cached by every node in the route. The accumulated paths information is used to route packets, the packets has the addresses of where it has to traverse. This may leads to overhead for long path to traverse; to avoid this DSR contains a flow id, which will forward packets with multi-hop basis. All the routing information is updated in mobile nodes.

The destination node unicasts the best route the one received first and caches the other routes for future use. A route cache is maintained at every node so that, whenever a node receives a route request and finds a route for the destination node in its own cache, it sends a packet itself instead of broadcasting.

The way that the route maintenance mechanism works is described below. Whenever a node finds out a link break via link layer acknowledgements or hello messages, it broadcasts a packet in a way similar to DSR to notify the source and the end nodes. If the link between nodes C and F breaks on the path A-C-F-G, packets will be sent by both F and C to notify the source and the destination nodes.

The main advantage of AODV is the avoidance of source routing to reduce the routing overload in a large network. Another good feature of AODV is its application of expanding-ring-search to control the flood of packets and search for routes to unknown destinations. In addition, it also supplies destination sequence numbers, allowing the nodes to have more up-to-date routes.

In this paper we model a performance evaluation of privacy protocols for Information Centric Networking (ICN). It is divided into three-fold: First, we describe a performance framework for comparing current and future solutions. Second, we assume and prove the existence of unsafe replicas, cached content that remains available to users whose access has been revoked. Third, we propose a performant protocol that solves the problem of unsafe replicas without tampering with the caching functionality of ICN.

3. PROBLEM DEFINITION

Trace files can document every event that occurred in the simulation and are used for analysis. Certain simulators have added functionality of capturing this type of data directly from a functioning production environment, at various times of the day, week, or month, in order to reflect average, worst-case, and best-case conditions.

Need for system:

Network simulators use discrete event simulation, in which a list of pending events is stored, and those events

P-ISSN: 2347-4408
E-ISSN: 2347-4734

are processed in order, with some events triggering future events such as the event of the arrival of a packet at one node triggering the event of the arrival of that packet at a downstream node.

4. PROPOSED SYSTEM

Hybrid Dynamic Energy Routing Protocol (HDERP) is reliable, has higher life span and uses energy efficiently, by which efficiency of overall network increases. The main aim of this paper is to minimize the time delay in delivering the packets from one end to other end and energy consumption. HDERP addresses three important requirements of ad hoc networks: energy-efficiency, reliability, and prolonging network lifetime.

HDERP, on the other hand, is an energy-efficient routing algorithm which finds routes minimizing the total energy required for end-to-end packet traversal. HDERP are proposed for networks in which either hop-by-hop or end-to-end retransmissions ensure reliability.
Hybrid Cryptography provides the hybrid cryptography method. Main objective of paper is exploring way of encryption done to improve some aspects of the algorithm which is already existed and create way for the excellent security.

4.1 Advantages

- Combining two security features then improve security enhancements
- Enhanced Attackers detection and prevention
- Throughput and packet delivery ratio can be improved
- reliability increases

4.2 Modules

Modules of our project are,

i. MANET Network Deployment
ii. Data Communication
iii. HDERP

4.3 Data Flow Diagram

The data flow diagram DFD is one of the most important modeling tools. It is used to model the system components. These components are the system process, the data used by the process, an external entity that interacts with the system and the information flows in the system.

4.4 Input Design

Input design is the process of converting the user-originated data into a computer-based format. Inaccurate input data are the most common cause of error in data processing. The goal of an input data are collected and organized into a group and error free. Input data are collected and organized into a group of similar data. Once identified, appropriated input media are selected for processing.

4.4.1 Unit testing

Unit testing focuses on verification errors on the smallest unit of software design-the module. Using the procedural design description as a guide, important control paths are tested to uncover errors within the boundary of the module.

5. PERFORMANCE EVALUATION

The software is completely built, a series of acceptance tests are conducted to enable the client to validate all requirements. The user conducts these tests rather than the system developer, which can range from informal test drive to a planned and systematical executed series of tests.

6. CONCLUSION AND FUTURE WORK

We proposed a unified trust management scheme that enhances the security of MANET. More nodes should be involved in the network to prevent, detect, and respond to the hacking attacks. Detecting attack in the destination node is accurate, but attack taken place in source node is difficult to find, and the detecting attack at the source node is the best option to secure the network from malicious attacks. All nodes in the network should be authenticated so that malicious users could be identified and their activities can be suppressed. Misbehaviors such as dropping or modifying packets can be detected in our scheme through trust values by direct and indirect observation. Nodes with low trust values will be excluded by the routing algorithm. Therefore, secure routing path can be established in malicious environments. In our proposed system preventing and detecting hacking attacks over network packets should be observed. Another factor is that packets may be dropped in the neighbor nodes if the packets get buffered in the queues. Our System increases the efficiency and performance of the packet delivery from source to destination nodes. In our future work, we will extend the proposed scheme to MANET with cognitive radios.

References

[1] R. Badonnel, R. State, and O. Festor. Self-configurable fault monitoring in ad-hoc networks. Ad Hoc Networks, 6(3):458–473, May 2008.
[2] P. Bahl and V. N. Padmanabhan. RADAR: An in-building RF-based user location and tracking system. In Proc. of IEEE INFOCOM, 2000.
[3] Y. Bar-Shalom, T. Kirubarajan, and X.-R. Li. Estimation with Applications to Tracking and Navigation. John Wiley & Sons, Inc., 2002.
[4] D. Ben Khedher, R. Glitho, and R. Dssouli. A Novel Overlay-Based Failure Detection Architecture for MANET

P-ISSN: 2347-4408
E-ISSN: 2347-4734

Applications. In IEEE International Conference on Networks, pages 130–135, 2007.
[5] C. Bettstetter. Smooth is Better than Sharp: A Random Mobility Model for Simulation of Wireless Networks. In Proc. of ACM International Workshop on Modeling, Analysis and Simulation of Wireless and Mobile Systems, pages 19–27, New York, NY, USA, 2001. ACM.
[6] C. Bettstetter. Topology Properties of Ad Hoc Networks with Random Waypoint Mobility. ACM SIGMOBILE Mobile Computing and Communications Review, 7(3):50–52, 2003.
[7] J. Broch, D. A. Maltz, D. B. Johnson, Y.-C. Hu, and J. Jetcheva. A Performance Comparison of Multi-Hop Wireless Ad hoc Network Routing Protocols. In Proc. of MobiCom, pages 85–97, New York, NY, USA, 1998. ACM.
[8] T. D. Chandra and S. Toueg. Unreliable Failure Detectors for Reliable Distributed Systems. Journal of the ACM, 43:225–267, 1996.
[11] I. Constandache, R. R. Choudhury, and I. Rhee. Towards Mobile Phone Localization without War-Driving. In Proc. of IEEE INFOCOM, March 2010.
[12] K. Dantu, M. H. Rahimi, H. Shah, S. Babel, A. Dhariwal, and G. S. Sukhatme. Robomote: enabling mobility in sensor networks. In Proc. of IEEE/ACM IPSN, 2005.
[13] M. Elhadef and A. Boukerche. A Failure Detection Service for Large-Scale Dependable Wireless Ad-Hoc and Sensor Networks. In International Conference on Availability, Reliability and Security, pages 182–189, 2007.
[14] K. Fall. A delay-tolerant network architecture for challenged internets. In Proc. of ACM SIGCOMM, pages 27–34. ACM, 2003