ISSN No:-2456 – 2165

Security Analysis and Improvements on Authentication Schemes for Network Coding

SanthanaLakshmi B,
M.E Student,
Kingston Engineering College.

Anitha.M M.E,
Asst Prof,
Kingston Engineering College.

Abstract— Network communication is a process is getting connected with more than one node. The communication gets established as by the term of server end or through number of connecting devices. The connecting devices may be routers, switches, gateway, access point etc. Each and every used to get communicate between the nodes. The communication occurs as a wired or wireless connection. The devices helps in term of all the way to get connected with nodes in term of making the devices to be connected for establishing the communication that in term turn the normal communication into a way of secured one. The devices act as a one that establishes the communication between numbers of node to deviate the connection problem that normally occur at the connected network. Data get shared between different nodes look for the connection to be established as a new one or to be check for the old one to be connected without any connection failure. Creating a new connection in a network is an easier one compared with checking for the connection failure in an older one. The connection is identified in term of data occur while passing the data through a particular path. The data get shared through a path which gets generated by the authorized server for the authorized user of the particular network.

Keywords—Network Split, Encoding, Decoding

I. INTRODUCTION

The complexity of the network occurs in term of connecting the nodes or passing the data in a connected path. The data get shared between the connected nodes are very complex in term of security problem get occur. The data get selected from the server end need to get reach each and every node of the network. The network looks for connection to be established from the routers which act as a connecting device between the numbers of nodes. The earlier system look for the connection and service needs to get done only by the server in term of authorized communication and valid reach of the data at each and every node end. The system unable to concentrate on both the process that leads to failure at communication level or at the security level. To solve these types of issues the system looks for a separate process to be done for the communication and security. The proposed system separates the communication to be done by the server end and the connection to be established by the routers. The routers provide the communication path to the number of clients connected in the network. The communication is provided as a both wired and wireless communication so that the communication can be done at different places without any connection between the nodes. The nodes acts as a client end to receive the data get transfer from the server end. The communication process get handled by the router where as the data get shared by the server end. The server end gets monitored by the routers and the client looks for data get shared by the server end. The communication failure overcome by separating the process and the path will be generated as a direct communication by the server to the client end.

II. EASE OF USE

The problem of controlling spreading processes in complex networks is also a thriving avenue for research. to formulate and solve optimal resource allocation problems that can be generalized to a large number of models including the SIS model. Furthermore, our framework allows us to simultaneously optimize the distribution of multiple types of control resources. The scope of the project is to implement the schemes that are introduced newly to overcome the drawbacks that are derived earlier and to overcome the upcoming drawback on prediction basis.

III. RELATED WORK

A lot of work focuses on establishing confidential communication links without using a secret key. These schemes are designed to obtain a positive secrecy rate without using any pre-shared key between two legitimate nodes. However, it is not guaranteed that such a scheme is always feasible. As another approach of physical-layer security, the secret key generation has been researched, which exploits the randomness and the reciprocity of the wireless channels to generate a secret key? If the eavesdroppers are located far enough from the legitimate nodes, e.g., more than half of the wavelength, the legitimate users experience independent channels to eavesdroppers, which enable to generate a secret key at legitimate nodes.

A. Abbreviations and Acronyms

a). AES:

AES is a symmetric block cipher. The key get generated by the server end get assigned to each and every packet that get generated in term of hyper split. The hyper split process divide the data into number of packets for security purpose. The packet get shared between the client end in different which make the intruders and hackers to be get confused where the packet get shared. The shared packets get separated between number of clients available at the server end via routers. The router looks for packet sharing between the networks client available at the server end. The server look for the data to shared without any failure in security. For the security process the server end look for the AES encoding process. The plain data get from the server end is generated to a cipher text by making use of the AES encoding process. The process gets the plain text a input and generate the cipher text as the output.

b). DSA

DSA propose in this system is to generate digital signature for each and every packet that get generate after the process of hyper split. The packets are unique so that they are transferred and accessed uniquely by both the server end and the client end. The client side looks for the valid key to be assigned for the packet that lead to proper communication of packets from the server end. The server end divides the packet with the help of hyper split and assign signature with the help of DSA to avoid security issues. The problem of security gets solved and both individual and overall in term of providing separate signatures for each and every packet available at the server end.

B. Equations

Key Size: [8]
Generated prime numbers p and q

p: [139]
q: [151]
The public key is the pair (N, E) which will be published.

N: [20989]
E: [1423]
The private key is the pair (N, D) which will be kept private.

N: [20989]
D: [17587]
Please enter message (plaintext):
aaaa
Ciphertext: [193C 4A9E 44 90D 3DA8 F18]
6460 19102 68 2317 15784 3864
big[Ljava.math.BigInteger;@1d9dc39

D: [17587]
N: [20989]
Recovered plaintext: [aaaaa]

C. Some Common Mistakes

The system checks for the file that has been selected by the node to be forwarded. The shortest path selection is later made by the server end in order to create path for communication between one to another in term of data sharing. The data is send to number of intermediate nodes and the communication get enabled and processed by the routers. The routers check for the connection failure and make the node to engaged at the time of data forwarding. The data get forwarded through the intermediate node get enlarged while at the receiver end.

IV. IMPLEMENTATION

In the Proposed System, some new enhanced cryptographic mechanisms may be adopted in order to provide an enhanced security at frame level especially regarding the added data consumption and misuse, by managing both encryption and integrity control into a unique processing. Good candidates may be taken from Determinist Authenticated Encryption Scheme. A message that includes the useful frame content and that can include an added context header, whose content is built for example with shared and non-transmitted signaling data. Privacy is compromised only to the extent that some minimal amount of information is revealed: the almost information that may be revealed is the fact that the plaintext of a frame is equal to the plaintext of a prior frame. In addition, it is revealed only when the plaintext and the header content are equal over two frames. The data get passed through un-trusted relay in order to reduce the waiting process for trusted relay. The pilot signal gets passed between sender-receivers before the data transmission.

Modules:

- Network configure
- Hyper split
- Secure analysis

A. Network configures:

This module creates network structure such as server, client and some intermediate nodes. All Nodes are inter connected like wireless sensor network. A wireless sensor network (WSN) of spatially distributed autonomous sensors to *monitor* physical or environmental conditions, such as temperature, sound, pressure, etc. and to cooperatively pass their data through the network to a main location. The more modern networks are bi-directional, also enabling *control* of sensor activity. The development of wireless sensor networks was motivated by military applications such as battlefield surveillance; today such networks are used in many industrial and consumer applications, such as industrial process monitoring and control, machine health monitoring, and so on.

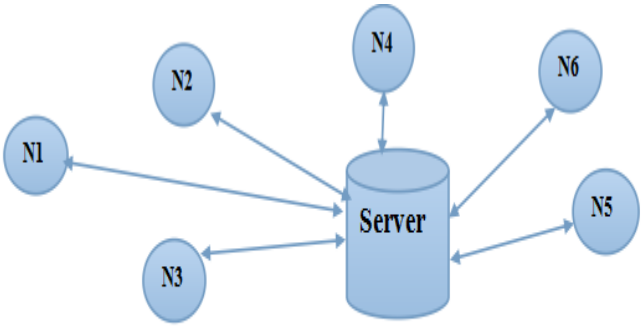

Fig. 1: Network Configure

B. Hyper split

To fill the gap between theory and practice, in this paper, we propose a novel packet classification algorithm named Hyper Split. Compared to the well-known HiCuts and HSM algorithms, Hyper Split achieves superior performance in terms of classification speed, memory usage and preprocessing time. The practicability of the proposed algorithm is manifested by two facts in our test: HyperSplit is the only algorithm that can successfully handle all the rule sets.

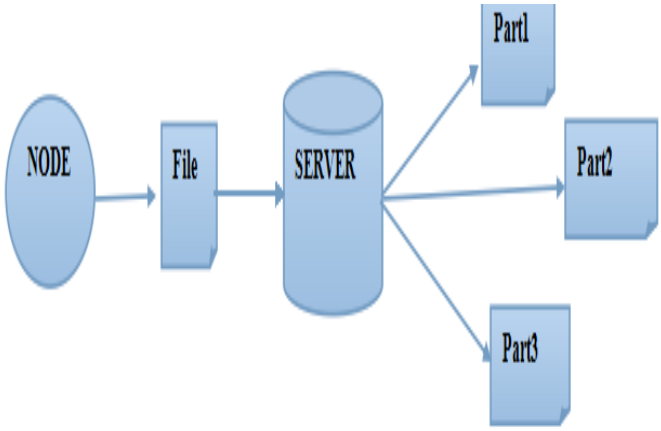

Fig.2: Hyper Split

C. Secure analysis

The security analysis module checks for the security level at each and every level of the client end while the data get transferred from the server end. The server end search for the data and the data get shared by the router path to each and every client end avail at the network. The network connected by the router check for the security issue to avoid the data loss, data mismatches , data aggregation problem that occur as a common issue at the inter or intra connected network.

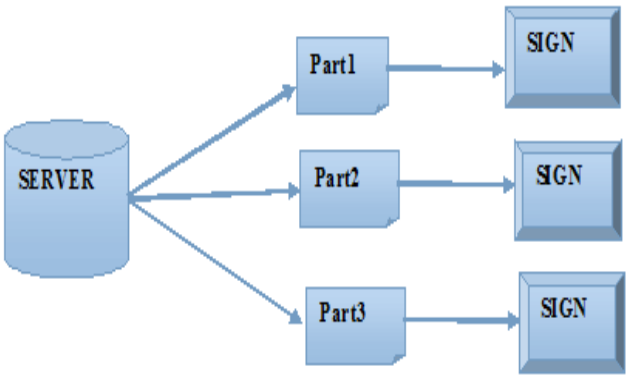

Fig. 3: Secure Analysis

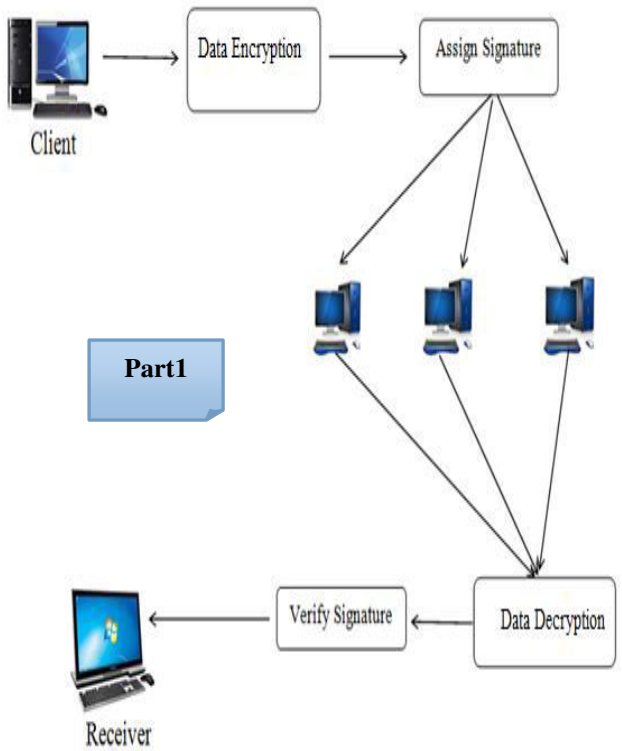

Fig. 4: System Process Diagram

This diagram describes the functionality of the proposed system. The system checks for the file that has been selected by the node to be forwarded. The network coding is applied by the server for clear view of the data to be shared in the secured way. The data get shared by the user via intermediate node is at risk of data leakage. To avoid these type of issues the data get packets into multiple one that are provided with individual signatures so that the data get shared by the user will monitored and get forwarded in a proper way. The receiver end receives the signature first after that the data get received by the user based on the signature. The signature act as a key for each and every packet to reduce the hacking of the packet from the anonymous user's of the connected network.

REFERENCES

[1]. R. Ahlswede, N. Cai, S.-Y. R. Li and R. W. Yeung, "Network information flow," IEEE Transactions on Information Theory, vol. 46, no. 4, pp. 1204-1216, Jul. 2000.
[2]. D. Lun, M. Medard, R. Koetter, and M. Effros, "Further results on coding for reliable communication over packet networks," in Proceedings of IEEE International Symposium on Information Theory (ISIT), pp. 1848-1852, Sep. 2005.
[3]. J. Widmer and J.-Y. Le Boudec, "Network coding for efficient communication in extreme networks," in Proceedings of the ACM SIGCOMM workshop on Delay-tolerant networking, pp. 284-291, Aug. 2005.
[4]. S.-Y. Li, R. Yeung, and N. Cai, "Linear network coding," IEEE Transactions on Information Theory, vol. 49, no. 2, pp. 371-381, Feb. 2003.
[5]. R. Koetter and M. Medard, "An algebraic approach to network coding," IEEE/ACM Transactions on Networking, vol. 11, no. 5, pp. 782-795, Oct. 2003.
[6]. J.-Q. Jin, T. Ho, and H. Viswanathan, "Comparison of network coding and non-network coding schemes for multi-hop wireless networks," in Proceedings of IEEE International Symposium on Information Theory (ISIT), pp. 197-201, Jul. 2006.
[7]. Y.Wu, P. Chou, and S.-Y. Kung, "Minimum-energy multicast in mobile ad hoc networks using network coding," IEEE Transactions on Communications, vol. 53, no. 11, pp. 1906-1918, Nov. 2005.
[8]. F. Cheng and R. W. Yeung, "Performance bounds on a wiretap network with arbitrary wiretap sets," IEEE Transactions on Information Theory, vol. 60, no. 6, pp. 3345-3358, Jun. 2014.
[9]. Z. Zhang, "Network error correction coding in packetized networks," in IEEE Information Theory Workshop, pp. 433-437, Oct. 2006.
[10]. N. Cai and R. W. Yeung, "Network coding and error correction," in Proceedings of IEEE International Symposium on Information Theory (ISIT), pp. 119-122, Oct. 2002.