ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Special Issue 2, March 2018

Dynamic Repeating With Secured Multipath Batch Configuration

N.Jaswanthi[1], B.Ramya[2], V.Vyshnavi[3], S.Aiswarya[4]

UG Student, Department of Computer Science and Engineering, Velammal Institute of Technology, Chennai, Tamil Nadu, India[1]

UG Student, Department of Computer Science and Engineering, Velammal Institute of Technology, Chennai, Tamil Nadu, India[2]

UG Student, Department of Computer Science and Engineering, Velammal Institute of Technology, Chennai, Tamil Nadu, India[2]

Assistant Professor, Department of Computer Science and Engineering, Velammal Institute of Technology, Chennai, Tamil Nadu, India[4]

ABSTRACT: Wireless Mobile Networks (WMNs) have been dramatically developed due to the proliferation of inexpensive, widely available wireless mobile devices. With the increasing number of mobile applications, such as social media networks, GPS, yelp, etc., people's life has been inseparable from mobile devices which can access the Internet at anytime and anywhere. However, due to the openness characteristic of wireless channels, it becomes easier for malicious nodes to interfere the access process by tampering or forging request messages.To protect the security of access, one effective approach is to sign each outgoing message with a digital signature, and let the destination verify each received signature .The Data Sender will first split the packets into multiple batches and create Batch signature for every batch and then starts sending the packets to the destination. As it is Wireless network, multiple nodes has to transmit the data in the given network. If any node tries to inject any packet or remove any packet its ID will also be added to the Batch Signature. Verifier first verifies the signature information before transmitting the packets to the destination. We also implement node energy level estimation in order to verify whether the same node transmitting the data or not. Before transmission of packets the routes and the nodes are identified. Every node's ID and relevant Energy level is verified before transmitting the packets. If any variation, then packets are discarded so that malicious packets are not transmitted.

KEYWORDS: Dynamic rerouting, Energy level monitoring, Batch Identification Game Model, Batch Signature.

I. INTRODUCTION

Network security is the emerging technology domain which consists of the policies and practices adopted to prevent and monitor unauthorized access, misuse, modification, or denial of a computer network and network-accessible resources. Network security involves the authorization of access to data in a network and provides protection to data against hacking which is controlled by the network administrator. Users choose or are assigned an ID and password or other authenticating information that allows them access to information and programs within their authority. Network security includesa variety of computer networks, such aspublic data, private data, sensitive data and confidential data. It provides secure transactions and communications among businesses, government agencies and individuals. Networks can be private, such as within a company, and others which might be open to public access. Network security is involved in organizations, enterprises and other types of institutions to provide privacy and integrity among the organizations. It does as its title explains: It secures the network, as well as protecting and

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Special Issue 2, March 2018

overseeing operations being done.The most effective of protecting a data in a network is by assigning it a unique ID and a corresponding password key.

To protect the security of access, one effective approach is to sign each outgoing message with a digital signature, and let the destination verify each received signature. Generally, signature verification induces extra delay and computational cost. The traditional way that verifying messages signatures individually could induce tremendous delay and severely affect the Quality of Service (QoS), especially when network traffic is heavy and a large number of signatures need to be verified.To reduce verification delay, the proposal of batch cryptographic technique is introduced, which is a promising way in computer network security.

The concept of batch cryptography was introduced by Fiat in 1990 for an RSA-type signature for providing processes like encryption, decryption and key exchange. The first efficient batch verifier was proposed by Naccache et al in 1994 for DSA-type signatures. The Batch cryptography mainly focus on two directions: batch verification and batch identification. Batch verification deals with n (message, signature) pairs as a batch at a time instead of one by one. As a result, compared with the traditional way, the validity of a batch can be checked more efficiently, and the verification delay can be remarkably reduced. Batch verification methods return true if all of the n signatures are valid, and false when there is any invalid signatures. Considering that the verification of massive messages may induce huge time and cost in mobile networks, proposal of an efficient identity-based batch verification scheme to reduce the delay in network coding. A batch signature verification scheme for the communications between mobile nodes and the infrastructure to lower the total verification time is introduced. A group signature and batch verification method is used for providing secure pseudonymous authentication in VANET. Unfortunately, the performance may be severely affected if there are invalid signatures existing in the verified batch, even though the schemes protect the authenticity of messages. Adversaries can negate the advantages of batch verification by polluting signatures within a batch. It is unrealistic to completely prevent all adversaries from generating false messages with invalid signatures. Thus, to make the efficient performance of batch verification, we should identify invalid signatures in a batch rapidly. Batch identification is a technique to find the bad signatures within a batch when the batch verification fails. Due to the inefficiency of individual data node ID, divide-and-conquer techniques have been proposed to improve the performance of batch identification. Those methods can significantly reduce the identification time at different levels. Existing batch identification algorithms have been developed into two main branches: special and generic. The special methods are designed for certain batch signature types such as RSAtype, DSA-type, and pairing-type. Lee et al. proposed a method to identify bad signatures in RSA-type batches. Later, Law and Matt presented a quick binary and exponentiation method to find invalid signatures. Stanek showed that the method in was flawed, and proposed an improved protocol to resist attacks.Matt discussed a solution in pairing-based signature scheme, which can identify nontrivial numbers of invalid signatures in batches.

Though these works are state of art, it is challenging to apply them with various batch verification algorithms. The batch identification model are utilized to group testing technique to find invalid signatures. A divide-and-conquer technique algorithm, which splits an data into sub batch problems recursively, until all invalid signatures are identified. Zaverucha et al presented and compared some group testing algorithms for finding invalid signatures. Zhang et al. adopted the group testing technique to find invalid signatures in a batch inmobile networks.

II. RELATED WORK

In 2016, J. Chen, K.He, Q. Yuan, R. Du, and J. Wu, Distributed greedy coding-aware deterministic routing for multi-flow in wireless networks. It has been proved that network coding can optimize routing in wireless networks. Thus, in deterministic routing, coding is considered as an important factor for route selection. While the existing deterministic routing solutions detect paths with coding opportunities based on the two-flow coding, little attention has been drawn to the multi-flow situation. Coding multiple flows *directly*, however, can improve the coding benefit when multiple flows intersect at coding nodes. In this paper, we analyze the challenges of the multi-flow coding, and propose a Greedy Multi-flow-based Coding-aware Routing (MuCAR) protocol in wireless networks. The main idea is to define the decoding policy and the coding condition in the multi-flow environment, and code the multiple intersecting flows in a

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Special Issue 2, March 2018

greedy way. Meanwhile, we discuss the interference issue in the multiflow coding and its solution. We show that MuCAR can induce competitive performance in terms of increased coding benefit and decreased delay, which is verified by extensive simulations

In 2016, Q. Wang, M.He, M. Du, S. S. M. Chow, R. W. F. Lai, and Q. Zou, Searchable encryption over feature-rich data. Storage services allow data owners to store their huge amount of potentially sensitive data, such as audios, images, and videos, on remote cloud servers in encrypted form. To enable retrieval of encrypted files of interest, many searchable symmetric encryption (SSE) schemes have been proposed. However, most existing SSE solutions construct indexes based on keyword-file pairs and focus on boolean expressions of exact keyword matches. Moreover, most dynamic SSE solutions cannot achieve forward privacy and reveal unnecessary information when updating the encrypted databases. We tackle the challenge of supporting large-scale similarity search over encrypted feature-rich multimedia data, by considering the search criteria as a high-dimensional feature vector instead of a keyword. Our solutions are built on carefully-designed fuzzy Bloom filters which utilize locality sensitive hashing (LSH) to encode an index associating the file identifiers and feature vectors. Our schemes are proven to be secure against adaptively chosen query attack and forward private in the standard model. We have evaluated the performance of our scheme on various real-world high-dimensional datasets, and achieved a search quality of 99% recall with only a few number of hash tables for LSH. This shows that our index is compact and searching is not only efficient but also accurate.

In 2015, J. Chen, K.He, R. Du, Y. Xiang, and Q. Yuan, Dominating set and network coding-based routing in wireless mesh networks. Wireless mesh networks are widely applied in many fields such as industrial controlling, environmental monitoring and military operations. Network coding is promising technology that can improve the performance of wireless mesh networks. In particular, network coding is suitable for wireless mesh networks as the fixed backbone of wireless mesh is usually unlimited energy. However, coding collision is a severe problem affecting network performance. To avoid this, routing should be effectively designed with an optimum combination of coding opportunity and coding validity. In this paper, we propose a Connected Dominating Set (CDS)-based and Flow-oriented Coding-aware Routing (CFCR) mechanism to actively increase potential coding opportunities. Our work provides two major contributions. First, it effectively deals with the coding collision problem of flows by introducing the information conformation process, which effectively decreases the failure rate of decoding. Secondly, our routing process considers the benefit of CDS and flow coding simultaneously. Through formalized analysis of the routing parameters, CFCR can choose optimized routing with reliable transmission and small cost. Our evaluation shows CFCR has a lower packet loss ratio and higher throughput than existing methods, such as Adaptive Control of Packet Overhead in XOR Network Coding (ACPO), or Distributed Coding-Aware Routing (DCAR).

In 2012, L. Xiao, Y. Chen, W. S. Lin, and K. J. R. Liu, Indirect reciprocity security game for large-scale wireless networks. Radio nodes can obtain illegal security gains by performing attacks, and they are motivated to do so if the illegal gains are larger than the resulting costs. Most existing direct reciprocity- based works assume constant interaction among players, which does not always hold in large-scale networks. In this paper, we propose a security system that applies the indirect reciprocity principle to combat attacks in wireless networks. Because network access is highly desirable for most nodes, including potential attackers, our system punishes attackers by stopping their network services. With a properly designed social norm and reputation updating process, the aim is to incur a cost due to the loss of network access to exceed the illegal security gain. Thus rational nodes are motivated to abandon adversary behavior for their own interests. We derive the optimal strategy and the corresponding stationary reputation distribution, and evaluate the stability condition of the optimal strategy using the evolutionarily stable strategy concept. This security system is robust against collusion attacks and can significantly reduce the attacker population for a wide range of attacks when the stability condition is satisfied. Simulation results show that the proposed system significantly outperforms the existing direct reciprocity-based systems, especially in the large-scale networks with terminal mobility. This technique can be extended to many wireless networks, including cognitive radio networks, to improve their security performance.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Special Issue 2, March 2018

In 2012, L. Y. Yeh, Y. L. Huang, A. Joseph, S. Shieh, and W. Tsaur, A batch-authenticated and key agreement framework for P2P-based online social networks. Online social networks (OSNs) such as Facebook and MySpace are flourishing because more and more people are using OSNs to share their interests with friends. Because security and privacy issues on OSNs are major concerns, we propose a security framework for simultaneously authenticating multiple users to improve the efficiency and security of peer-to-peer (P2P)-based OSNs. In the proposed framework, three batch authentication protocols are proposed, adopting the one-way hash function, ElGamal proxy encryption, and certificates as the underlying cryptosystems. The hash-based authentication protocol requires lower computational cost and is suitable for resource-limited devices. The proxy-based protocol is based on asymmetric encryption and can be used to exchange more information among users. The certificate-based protocol guarantees non repudiation of transactions by signatures. Without a centralized authentication server, the proposed framework can therefore facilitate the extension of an OSN with batched verifications.
In this paper, we formally prove that the proposed batch authentication protocols are secure against both passive adversaries and impersonator attacks, can offer implicit key authentication, and require fewer messages to authenticate multiple users. We also show that our protocols can meet important security requirements, including mutual authentication, reputation, community authenticity, non repudiation, and flexibility. With these effective security features, our framework is appropriate for use in P2P-based OSNs.

III. PROPOSED SYSTEM

Proposed secure batch verification with group testing to improve the real-time performance of mobile networks. Note that those generic methods are usually suitable for a specific attack situation in terms of the number of invalid signatures. Their performance may severely degrade if the number of invalid signatures varies, when the attack strategy is changed by the movement of adversaries or the alteration of false message attacking frequency. To select the most suitable data path, batch verification algorithm is proposed. However, they did not sufficiently consider the automatic selection of batch identification. Therefore, designing a generic and auto-match batch identification solution towards the heterogeneous and dynamic attack scenario becomes significant.
The proposal of Batch Identification Game Model (BIGM) is made, thus enabling nodes to identify invalid signatures with a reasonable delay under dynamic attacks. To enhance the flexibility of our model, we subdivide BIGM into Batch Identification Game Model with Complete information (C-BIGM) and Batch Identification Game Model with Incomplete information (I-BIGM) is used to protect regular nodes from the various attacks due to invalid signatures. In our model, a mobile node may be a regular one or a malicious one, and the game occurs between a regular node and its malicious neighbors. The regular node, as a verifier, aims at finding the invalid signatures to eliminate the impact of malicious nodes. The malicious neighbors, as attackers, intend to interpose batch verification process by broadcasting false messages signed by invalid signatures with different frequencies.

3.1 SOURCE ROUTING AND PACKET SPLITTING

In this, subsystem is developed in order to create a network construction. In a network, nodes are interconnected, which is monitoring all the other nodes. All nodes are sharing their information with each others. Node will be connected with each other to share know ID of next and previous node. In this user data will split into multiple packets with batch signature. Data should be splits and send into destination in secured way. Packet splitting is for security purpose. Because if we send data in single packet without any signature there is a chance to loss data or hackers will easily hack the information . So we spilt it and add signature to every packet.

3.2 BATCH SIGNATURE VERIFICATION

Every node have to know their neighbor's node ID. Before send data from source to destination each node will previously know about the ID of next node. If data is send from one node to another node it will verify its ID with existing ID .if it match with existing signature data will transfer to next node. If any packets are loss or added to it that new ID will be added and send to next node so that it will discard that node by verifying its ID.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Special Issue 2, March 2018

FIGURE 1 -BATCH SIGNATURE VERIFICATION

3.3 ENERGY LEVEL MONITORING

In this subsystem energy level of every node is identified and set route to that path. Because the energy level of node is important to transfer data. If low level energy node is selected to send data there is a chance to loss or delay to transfer the data . So we also identify the energy level of every node.

Identify Energy Level

FIGURE 2 -ENERGY LEVEL MONITORING

3.4 DYNAMIC ROUTING AND PACKET DELIVERY

In this subsystem node is constructed to transfer the data from source to destination.

Before send data, path is identified to transfer the information. If selected route contain any traffic problem dynamic source route is selected and send data through that dynamic route. After verifying node ID, energy level and batch signature, data will be transferred from source to destination. If it is not match with previous information data will not send to the destination.

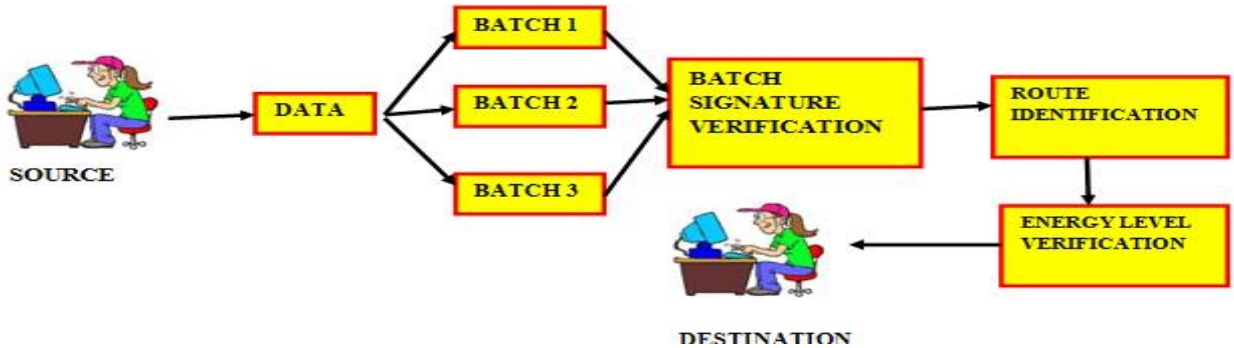

FIGURE 3 -DYNAMIC ROUTING AND PACKET DELIVERY

IV. RESULT AND ANALYSIS

Batch verification deals with n (message, signature) pairs as a batch at a time instead of one by one. As a result, compared with the traditional way, the validity of a batch can be checked more efficiently, and the verification delay can be remarkably reduced, Signature info before transmitting the packets to the destination. We also implement node energy level estimation in order to verify whether the same node transmitting the data or not. Before transmission of

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Special Issue 2, March 2018

packets the routes and the nodes are identified. Every node's ID and relevant Energy level is noticed by the verified before transmitting the packets. Batch verification methods return true if all of the n signatures are valid, and false when there is any invalid signature.

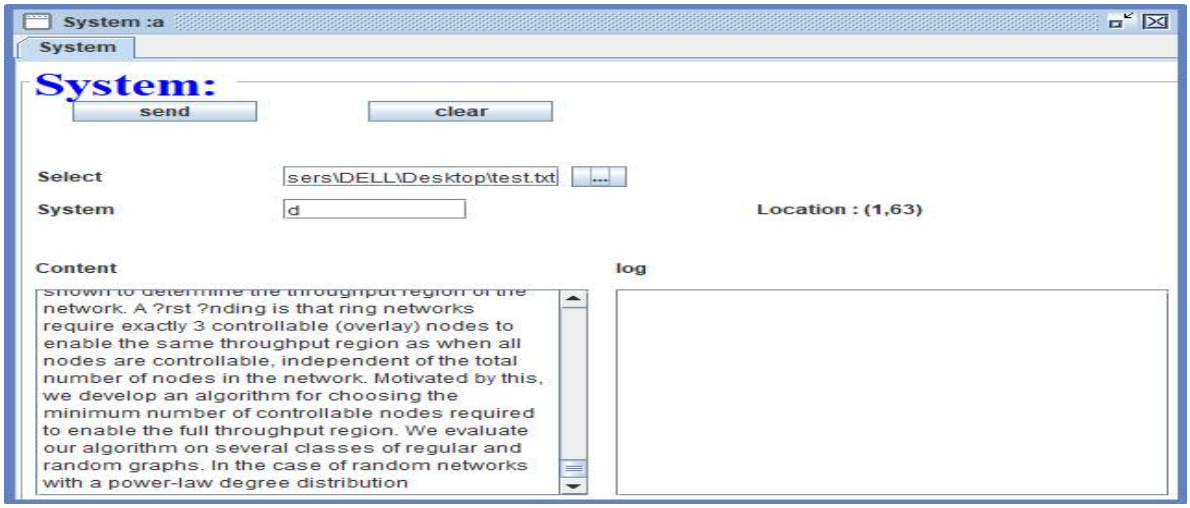

FIGURE 4- NODE AWITH DATA CONTENT

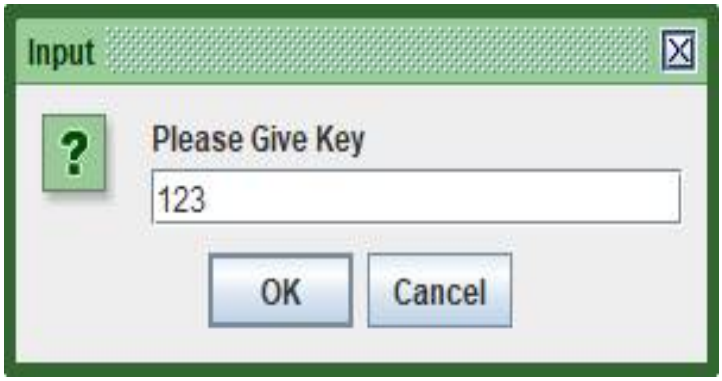

FIGURE 5 - ENCRYPTION OF DATA

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Special Issue 2, March 2018

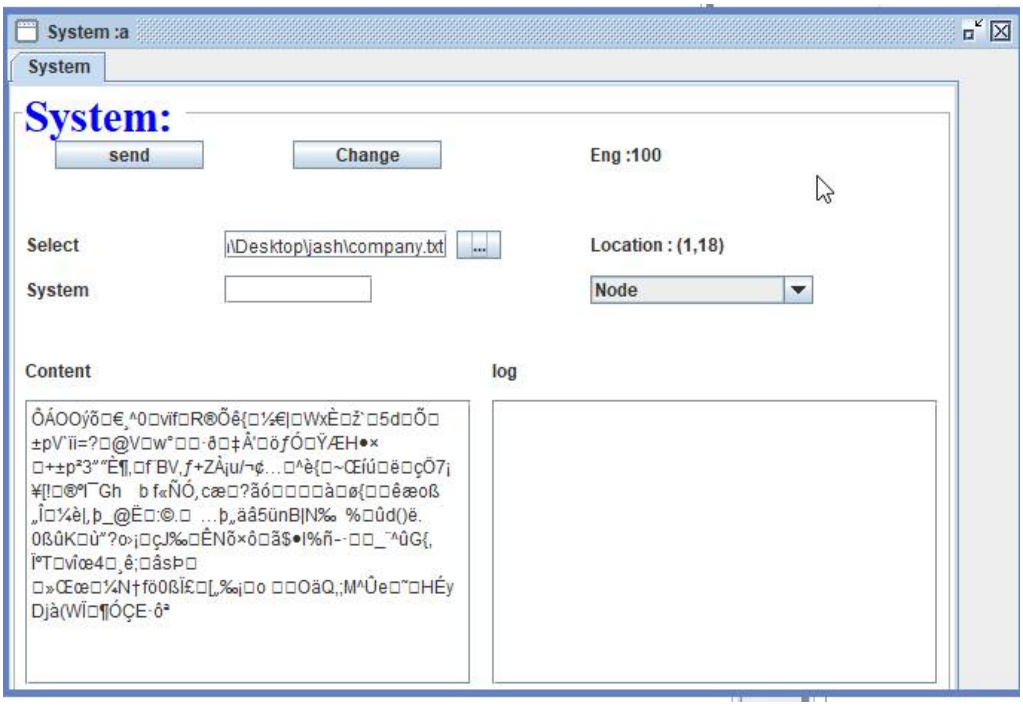

FIGURE 6 -ENCRYPTED FORM OF DATA

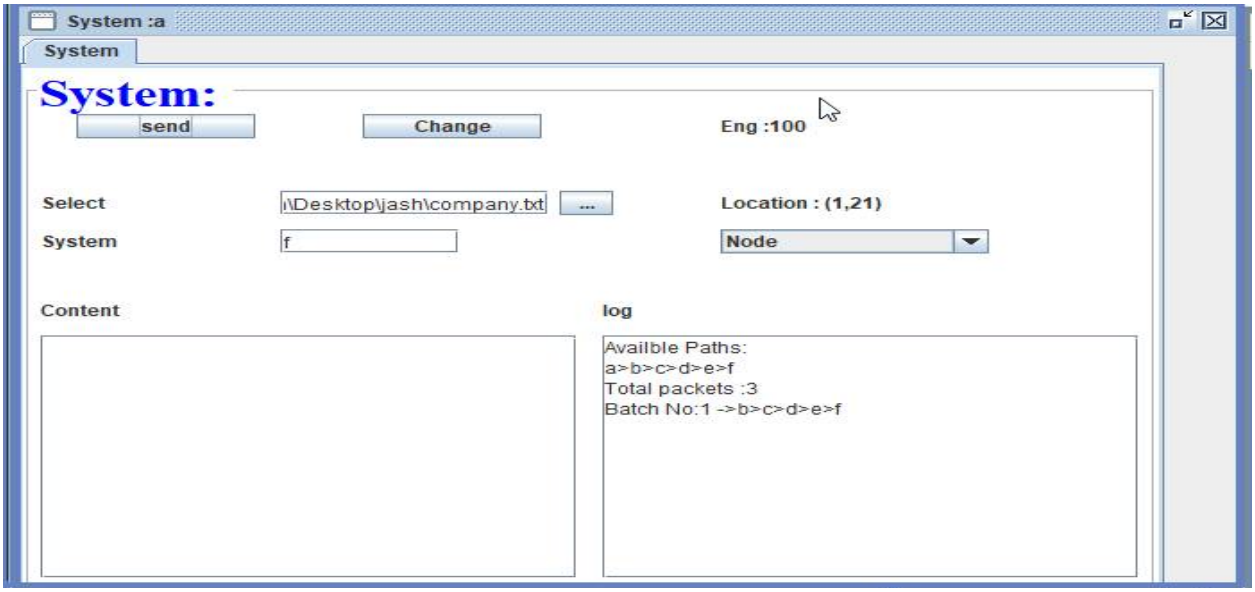

FIGURE 7 - SOURCE NODE a DISPLAYING THE AVAILABLE PATH

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Special Issue 2, March 2018

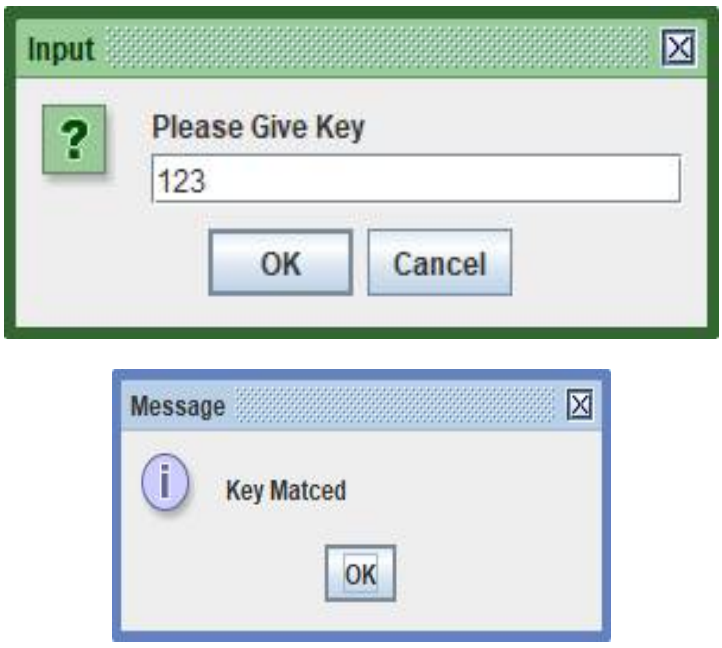

FIGURE 8 -DECRYPTION OF DATA

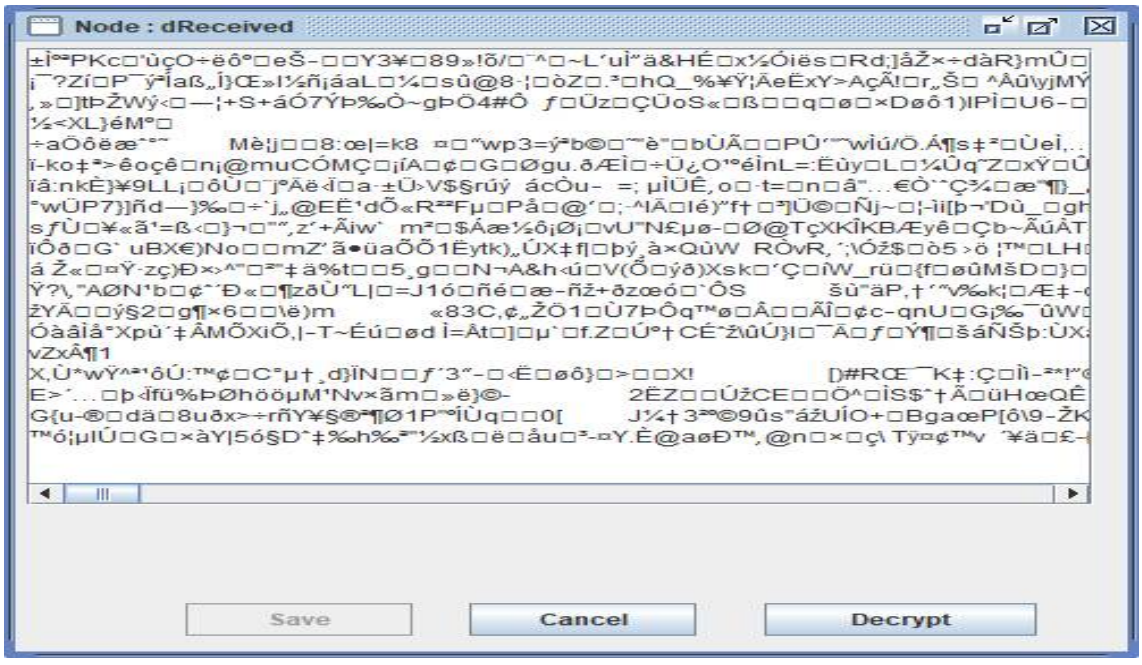

FIGURE 9 -DECRYPTED FORM OF DATA RECEIVED BY DESTINATION NODE

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Special Issue 2, March 2018

V.CONCLUSION

Thus the proposed system provides security to the data. Thus the attachment of sender signature with node ID is made. By this way intermediate node and receiver node can able to know who is the sender. If any interruption occurs while sending or if any hacker node tries to break the data, then the receiver can easily identify and block the hacker node. This can be made with the help of adjacent node in the desired path through mesh topology. So through this way, a secure data is transferred from sender to the receiver. Energy level of each node is analyzed and known prior.By this way,Optimal path is achieved.Secure data transmission occurs due to batch signature ID and encryption.

REFERENCES

[1] J. Chen, K. He, R. Du, Y. Xiang, and Q. Yuan, "Dominating set and network coding-based routing in wireless mesh networks," IEEE Trans. Parallel Distrib. Syst., vol. 26, no. 2, pp. 423–433, Feb. 2015.
[2] L. Xiao, Y. Chen, W. S. Lin, and K. J. R. Liu, "Indirect reciprocity security game for large-scale wireless networks," IEEE Trans. Inf. Forensics Secur., vol. 7, no. 4, pp. 1368–1380, Aug. 2012.
[3] J. Chen, K. He, Q. Yuan, R. Du, and J. Wu, "Distributed greedy coding-aware deterministic routing for multi-flow in wireless networks," Comput. Netw., vol. 105, pp. 194–206, 2016.
[4] M. Chen, Y. Hao, M. Qiu, J. Song, D. Wu, and I. Humar, "Mobilityaware caching and computation offloading in 5G ultradense cellular networks," Sensors, vol. 16, no. 7, pp. 974–986, 2016.
[5] Y. Liu, D. Bild, R. Dick, Z. Mao, and D. Wallach, "The Mason test: A defense against Sybil attacks in wireless networks without trusted authorities," IEEE Trans. Mobile Comput., vol. 14, no. 11,pp. 2376–2391, Nov. 2015.
[6] M. Chen, Y. Qian, S. Mao, W. Tang, and X. Yang, "Softwaredefined mobile networks security," Mobile Netw.Appl., 2016.[Online]. Available: http://doi:10.1007/s11036-015-0665-5.
[7] B. Alomair and R. Poovendran, "Efficient authentication for mobile and pervasive computing," IEEE Trans. Mobile Comput., vol. 13, no. 3, pp. 496–481, Mar. 2014.
[8] Q. Wang, M. He, M. Du, S. S. M. Chow, R. W. F. Lai, and Q. Zou, "Searchable encryption over feature-rich data," IEEE Trans. Depend. Secure Comput., 2016. [Online]. Available: http://doi.org/ 10.1109/TDSC.2016.2593444
[9] L. Y. Yeh, Y. L. Huang, A. Joseph, S. Shieh, and W. Tsaur, "A batch-authenticated and key agreement framework for P2P-based online social networks," IEEE Trans. Veh. Technol., vol. 61, no. 4, pp. 1907–1924, May 2012.
[10] K. He, J. Chen, R. Du, Q. Wu, G. Xue, and X. Zhang, "DeyPoS: Deduplicatable dynamic proof of storage for multi-user environments," IEEE Trans. Comput., 2016. [Online]. Available: http:// doi.org/10.1109/TC.2016.2560812
[11] A. Fiat, "Batch RSA," in Proc. Advances CRYPTO, 1989, pp. 175– 185. [12] D. Naccache, D. M'Raihi, S. Vaudenay, and D. Raphaeli, "Can DSA be improved? complexity trade-offs with the digital signature standard," in Proc. EUROCRYPT, 1994, pp. 77–85.
[13] J. Cheon, J. Coron, J. Kim, and M. Lee, "Batch fully homomorphic encryption over the integers," in Proc. EUROCRYPT, 2013, pp. 315–335.
[14] Z. Yu, Y. Wei, B. Ramkumar, and Y. Guan, "An efficient signaturebased scheme for securing network coding against pollution attacks," in Proc. IEEE INFOCOM, 2008, pp. 1409–1417.
[15] C. Zhang, R. Lu, X. Lin, P.-H. Ho, and X. S. Shen, "An efficient identity-based batch verification scheme for vehicular sensor networks," in Proc. IEEE INFOCOM, 2008, pp. 246–250.