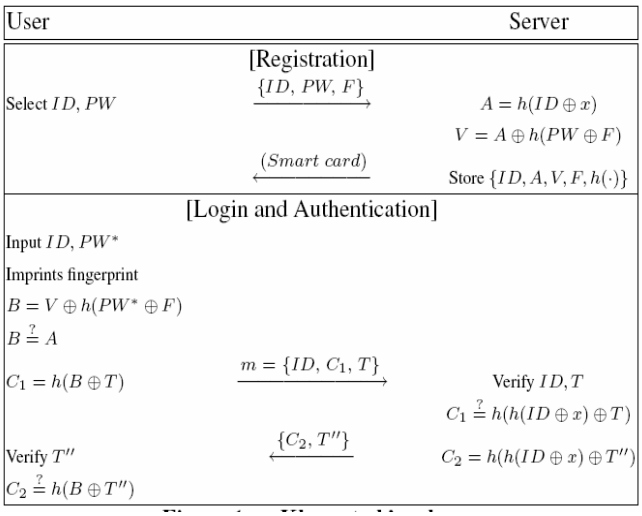
However, one weakness of their scheme is that a verification table should be maintained on the remote server in order to validate the legitimacy of the requesting users; if an intruder can somehow break into the server, the contents of the verification table may be easily modified. Therefore, many password authentication schemes have recognized this problem, and solutions based on smart cards have been proposed, where a verification table is no longer required.

In a typical smart card based password authentication scheme, remote users are authenticated with their smart cards as identification tokens. The card takes as input a password from the user, creates a login message from the given password, and sends the message to a remote server, which then checks the validity of the login message before allowing access to any services or resources. This way the administrative overhead of the authentication server is reduced, and the user only needs to remember his password.

Recently, some biometrics-based remote user authentication schemes have been designed. In 2002, Lee et al. proposed a fingerprint-based scheme using smart cards. It is based on ElGamal's public key cryptosystem, which also does not require password table for authentication. The scheme is novel in that biological information and two secret keys are employed to improve the security.

However, Lin et al. and Ku et al. pointed out in 2004 and 2005 respectively that Lee et al.'s scheme cannot withstand the masquerade attack, in which an adversary can impersonate a legitimate user without knowing the password and passing the fingerprint verification. Later, in ISPEC 2006, Khan et al. also showed that Lee et al.'s scheme was vulnerable to the server spoofing attack. Furthermore, they proposed an improved scheme to enhance the security. Based on the one-way hash function and fingerprint verification, Khan et al.'s scheme needs only to maintain one secret key, and a password verification table is not required on the server. They claimed that their scheme achieved mutual authentication between the user and the server, and thus eliminated the drawback of Lee et al.'s scheme. [1]



Content owners (such as authors and authorized distributors) are losing billions of dollars annually in revenues due to illegal copying and sharing of digital media. Digital rights management (DRM) systems are being deployed to address this problem. The user authentication, which is an essential part of a DRM system, determines whether a user is authorized to access the content. In a generic cryptographic system the user authentication is possession based. That is, possession of the decrypting key is a sufficient evidence to establish user authenticity. Because cryptographic keys are long and random, (e.g., 128 bits for the advanced encryption standard (AES), they are difficult to memorize. As a result, the cryptographic keys are stored somewhere (for example, on a computer or a smart card) and released based on some alternative authentication (e.g., password) mechanism, that is, upon assuring that they are being released to the authorized users only. Most passwords are so simple that they can be easily guessed (especially based on social engineering methods) or broken by simple dictionary attacks.

It is not surprising that the most commonly used password is the word "password"! Thus, the multimedia protected by the cryptographic algorithm is only as secure as the passwords (weakest link) used for user authentication that release the correct decrypting key(s). Simple passwords are easy to crack and, thus, compromise security; complex passwords are difficult to remember and, thus, are expensive to maintain.1 Users also have the tendency to write down complex passwords in easily accessible locations. [2]

Further, most people use the same password across different applications and, thus, if a single password is compromised, it may open many doors. Finally, passwords are unable to provide non repudiation; that is, when a password is shared with a friend, there is no way to know who the actual user is. This may eliminate the feasibility of countermeasures such as holding conniving legitimate users accountable in a court of law.

Many of these limitations of the traditional passwords can be ameliorated by incorporation of better methods of user authentication. Biometric authentication refers to verifying individuals based on their physiological and behavioral characteristics such as face, fingerprint, hand geometry, iris, keystroke, signature, voice, etc. It is inherently more reliable than password-based authentication, as biometric characteristics cannot be lost or forgotten (cf. passwords being lost or forgotten); they are extremely difficult to copy, share, and distribute (cf. passwords being announced in hacker websites) and require the person being authenticated to be present at the time and point of authentication (cf. conniving users denying having shared the password). [3]

Additionally, storing biometric information in repositories along with other personally identifiable information raises several security and privacy risks. These databases are vulnerable to attacks by insiders or external adversaries and may be searched or used outside of their intended purposes. It is important to note that if the stored biometric identifiers of an individual are compromised, there will be severe consequences for the individual because of the lack of revocation mechanisms for biometrics.

Due to the security and privacy problems of server side matching, there have been several efforts in biometric authentication technology using client side matching. Such an approach is convenient as it is relatively simple and cheap to build biometric authentication systems supporting biometric storage at the client end able to support local matching. Nevertheless, systems of such type are not secure if the client device is not trusted; therefore additional cryptographic support is need.

3. Proposed System

3.1 Setup Phase

In this module each node stores a unique identity and public/private key pair with a certificate, the public key of the AC, and the required cryptographic data for the key exchange protocol. Each node in a session has to share a symmetric key with the source node to compute the messages' keyed hash values. For efficient implementation, an identity-based key exchange protocol based on bilinear pairing can be used because the nodes do not need to exchange messages to compute the shared keys. The AC generates a prime p, a cyclic additive group (G), and a cyclic multiplicative group of the same order p such that an efficiently computable bilinear pairing. The source node initiates route establishment by broadcasting Route Request Packet (RREQ) that contains its identity (IDS), time stamp (TS), and the identity of the destination node (IDD) and the time to live (TTL). If the time stamp is within a proper range and the TTL is not zero, a network node decrements the TTL, appends its identity, and broadcasts the packet.

3.2 Data Generation

In this module, the source node initiates a packet series with maximum size by attaching its signature to the identities of the session nodes, TS, and VNS. This signature proves the source node's approval to pay for the session and authenticates its hash chain and links it to the session, i.e., the sender cannot deny generating the hash chain or initiating the session. In order to ensure the hop-by-hop message authenticity and integrity, the message's hash value can be included in the signature but with increasing the receipt size. Therefore, the source node attaches the hash series which contains a truncated keyed hash value for each node. Each intermediate node verifies the source node's signature to ensure that it will be rewarded for relaying the packets. Then, it verifies its message's truncated hash value to ensure the message authenticity and integrity and relays the packet after dropping its hash value. Each intermediate node saves the source node's signature and VNS to be used in the receipt composition.

3.3 ACK Generation

In this module, after receiving a data packet, the destination node sends back ACK packet containing a fresh hash value from its hash chain as an approval to pay for the message. Each intermediate node verifies that V_D is generated from hashing, and saves the last hash value to be used in the receipt composition

3.4 Receipt and Payment Redemption

In this module if the session is broken after receiving the first data packet, the intermediate nodes compose a receipt for receiving one packet. The payment data includes the identities of the payers and payees (R), the time of the transaction (TS), and the roots of the payers' hash chains. The security token is the hash value of the source and destination nodes' signatures. Attaching the hash of the signatures instead of the signatures can reduce the receipt size significantly. The security token can guarantee that the receipt is undeniable and unforgeable. Since the session is broken before receiving the ACK, the last released hash value from the destination node is V_D. If the last received packet is the ACK, the receipt is composed which is a proof for successfully delivering X messages.

In this module the network nodes periodically submit the receipts to the AC to redeem them. Once the AC receives a receipt, it first checks that the receipt has not been deposited before using the receipt's unique identifier, i.e., the identities of the nodes in the route and the establishment time. Then, the AC verifies the credibility of the receipt by generating the source and the destination nodes' signatures, and matching the signatures' hash value with the receipt's security token. Finally, the AC counts the packets' number from the hash chains' elements, and clears the receipt according to the rewarding and charging policy.

3.5 Enhanced Security

In this module, we enhance the use of public key cryptography by reapplying the security technique before sending the data packet from the source node and after receiving a data packet at the destination node, the destination nodes computes the decryption twice and based on the correctness, the destination node sends back ACK packet containing a fresh hash value from its hash chain as an approval to pay for the message. The enhanced technique also uses Secure Hash and Message Digest which is applied multiple times to protect the network with malicious nodes. The results and comparisons below clearly demonstrates that use of multiple SHA and MD-5 for HMAC will not form an additional overhead on the network as well as energy consumption is also negligible but we achieve higher security in terms of malicious node

4. Results

The concept of this paper is implemented and different results are shown below, the proposed paper is implemented in NS 2.34 on a Linux Fedora 10. The propose paper's concepts shows efficient results and has been efficiently tested on different Datasets. The Fig 1, Fig 2, Fig 3 and Fig 4 shows the real time results compared.

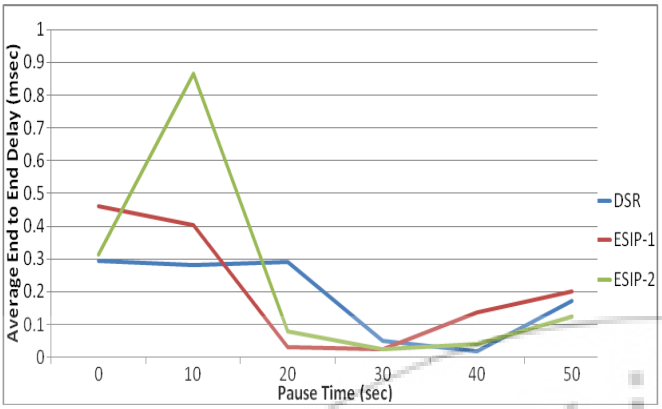


Figure 1: Average End to End Delay Vs Pause Time

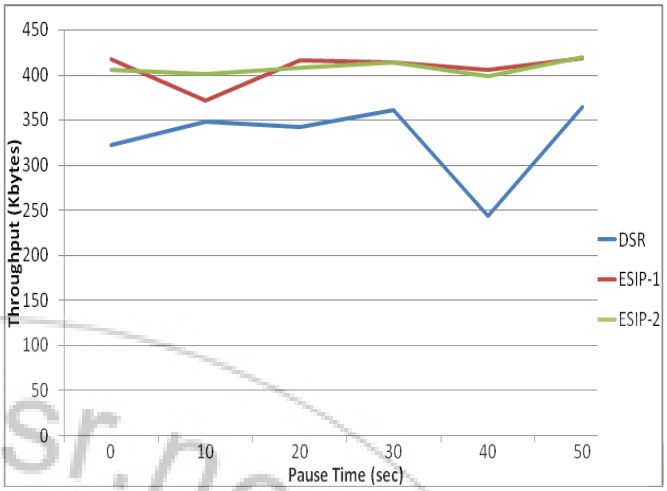


Figure 5: Throughput Vs Pause Time

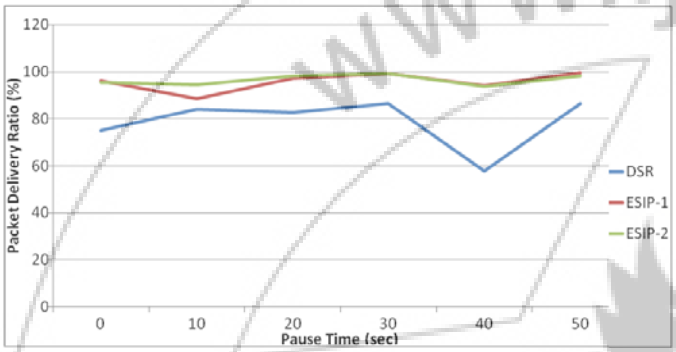


Figure 2: Packet Delivery Ratio to End Delay Vs Pause Time

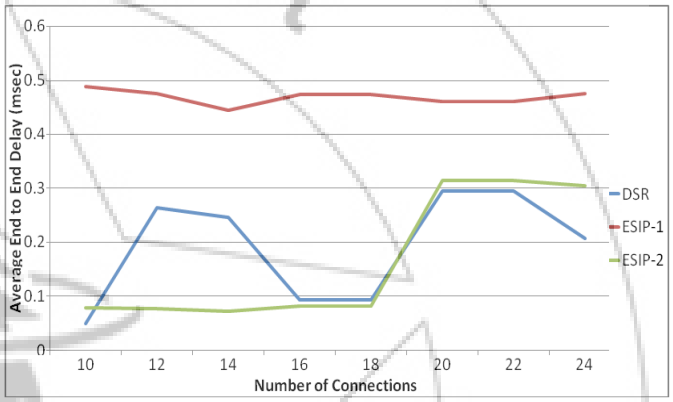


Figure 6: Average End to End Delay Vs Connections

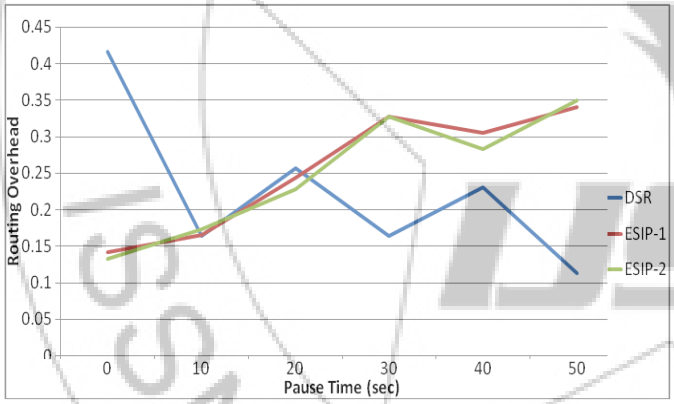


Figure 3: Routing Overhead Vs Pause Time

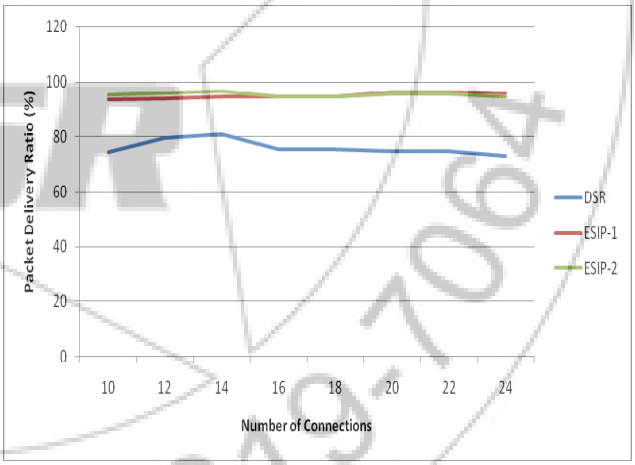


Figure 7: Packet Delivery Ratio Vs Connections

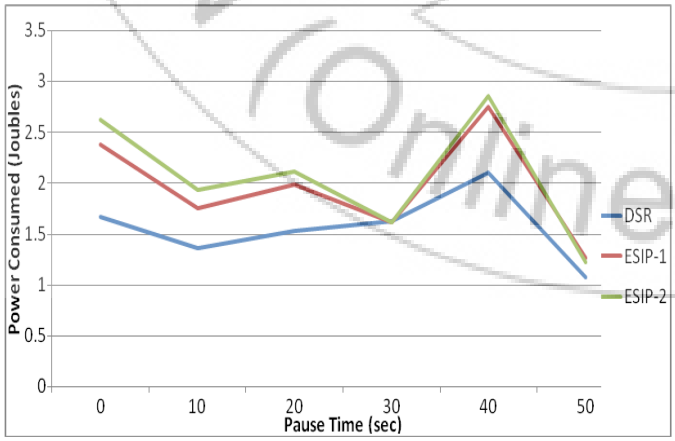


Figure 4: Power Consumption Vs Pause Time

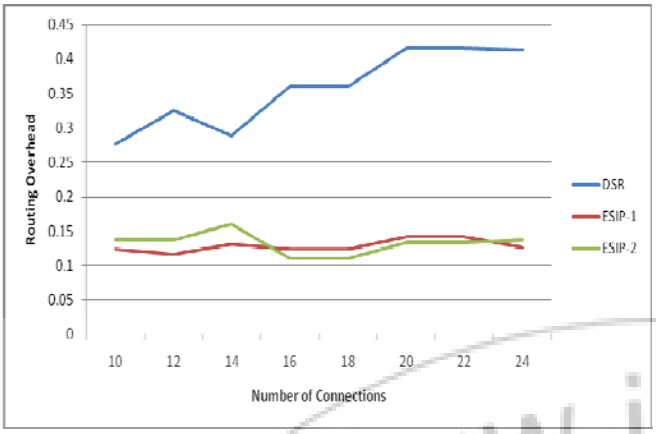


Figure 8: Routing Overhead Vs Connections

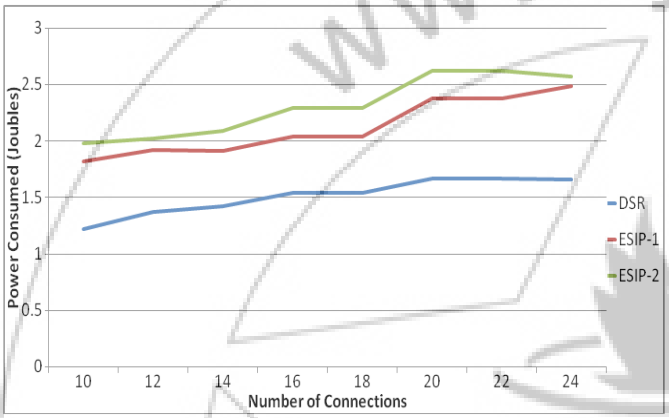


Figure 9: Power Consumed Vs Connections

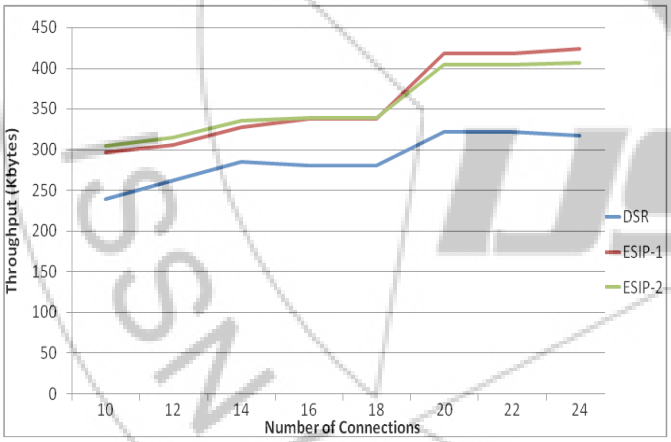


Figure 10: Throughput Vs Connections

5. Conclusion

In this paper, we have proposed secure cooperation incentive protocol with limited use of public-key cryptography for multihop wireless networks. The public-key operations are required only for the first packet and the efficient hashing operations are used in the next packets, so for a series of packets, the heavy overhead of the first packet vanishes and the overall overhead converges to that of the lightweight hashing operations. Our security analysis and performance evaluations have demonstrated that ESIP can secure the payment and improve the network performance significantly because the hashing operations dominate the nodes' operations.

6. Future Scope

The future scope of this proposed system is to extend the receipt format which can reveal the node at which the route was broken as well as we can also consider the irrational packet droppers and the reputation system should be carefully designed to identify the attackers in short time to reduce their harm and to avoid falsely identifying honest nodes as irrational packet droppers.

References

[1] G. Shen, J. Liu, D. Wang, J. Wang, and S. Jin, "Multi-Hop Relay for Next-Generation Wireless Access Networks," Bell Labs Technical J., vol. 13, no. 4, pp. 175-193, 2009.
[2] X. Li, B. Seet, and P. Chong, "Multihop Cellular Networks: Technology and Economics," Computer Networks, vol. 52, no. 9, pp. 1825-1837, June 2008.
[3] A. Abdrabou and W. Zhuang, "Statistical QoS Routing for IEEE 802.11 Multihop Ad Hoc Networks," IEEE Trans. Wireless Comm., vol. 8, no. 3, pp. 1542-1552, Mar. 2009.
[4] Y. Jiang, M. Shi, X. Shen, and C. Lin, "BAT: A Robust Signature Scheme for Vehicular Networks Using Binary Authentication Tree," IEEE Trans. Wireless Comm., vol. 8, no. 4, pp. 1974-1983, Apr. 2009.
[5] P. Gupta and P. Kumar, "The Capacity of Wireless Networks," IEEE Trans. Information Theory, vol. 46, no. 2, pp. 388-404, Mar. 2000.
[6] S. Marti, T. Giuli, K. Lai, and M. Baker, "Mitigating Routing Misbehavior in Mobile Ad Hoc Networks," Proc. IEEE/ACM MobiCom, pp. 255-265, Aug. 2000.
[7] D.B. Johnson, D.A. Maltz, and Y.C. Hu, "The Dynamic Source Routing Protocol for Mobile Ad Hoc Networks (DSR)," technical report, IETF MANET Working Group, Feb. 2007.
[8] P. Michiardi and R. Molva, "Simulation-Based Analysis of Security Exposures in Mobile Ad Hoc Networks," Proc. European Wireless Conf., Feb. 2002.

Author Profile

Barla. Bhavani obtained her B.Tech degree from J.B. Institute of Engineering and Technology, Yenkapally and Ranga Reddy District. Currently she is pursuing her M.Tech degree in Digital Systems and Computer Electronics. Her research interests are in the area in ADHOC and Wireless Sensor Networks, Advanced Data Communications, VLSI Design, Microcontroller Design, Real Time Operating Systems and Digital System Design.

Mrs.Thoomati Madhavi Kumari obtained B.Tech. in ECE and M.Tech. in Computer Science from JNT University. Presently Mrs. Madhavi is pursuing Ph.D. in Data security for natural languages using FPGA. Mrs. Madhavi joined the faculty of ECE Department of JNU College of Engineering, Kukatpally, Hyderabad as Assistant Professor and served the department for 13 years. Later she was appointed as Assistant Director, UGC-ASC, JNT University, and Hyderabad. She was associated with the implementation of AICTE Sponsored project on computer networks.