# Security Analysis and Performance Evaluation of an Enhanced Two-Factor Authenticated Scheme

Divya Jyoti
Department of Computer Science and Engineering
DAV Institute of Engineering and Technology, Jalandhar

Raman Kumar
Department of Computer Science and Engineering
DAV Institute of Engineering and Technology, Jalandhar

## ABSTRACT

Various security attacks may cause unauthorized access, misuse, modification, or denial of a computer network and network accessible resources. To prevent these attacks various authentication means can be used to provide authenticated key exchange protocols. Authenticated key exchange protocol allows the exchange of session key and also authenticates the identities of parties involved in the key exchange. It mathematically binds the agreed key to other agreed upon data such as shared secret keys, passwords and public/private key pairs. The reliability and security of the authentication protocol can be increased by combining two factors in the same authentication protocol. Many two-factor authenticated schemes have been proposed due to its usefulness. The main focus of this paper is to propose an enhanced two-factor authenticated scheme that can resist various security attacks in network by eliminating the attack races by matching it with knowledge available in the network as well as provide user anonymity.

## General Terms

Two-factor authentication, Security attacks.

## Keywords

Key exchange, Symmetric key, WSN, Authentication.

## 1. INTRODUCTION

Mostly security is based on cryptographic principles except for physical layer. It involves constructing and analyzing protocols that overcome the influence of adversaries. These protocols are related to various aspects in information security such as data confidentiality, data integrity, authentication and non-repudiation.

The main issue in cryptographic security is key management means how to exchange keys or other information so that no one else can obtain a copy. If sender and receiver want to exchange encrypted messages, each must be equipped to encrypt messages to be sent and decrypt messages received. The nature of the equipping they require depends on the encryption technique they might use. If they use a code, both will require a copy of the same codebook. If they use a cipher, they will need appropriate keys. If the cipher is a symmetric key cipher, both will need a copy of the same key. If an asymmetric key cipher with the public/private key property, both will need the other's public key. Key exchange protocols are used by which cryptographic keys are exchanged between users, allowing use of a cryptographic algorithm. Key exchange protocols allow two or more parties communicating over a public network to establish a common secret key called a session key. Due to their significance in building a secure communication channel, a number of key exchange protocols have been suggested over the years for a variety of settings. We can use various authentication means to provide authenticated key exchange in order to prevent man-in-the-middle attack and related attacks.

### 1.1 Two-Factor Authentication

Two-factor authentication requires the use of two authentication factors. The most commonly used authentication factors in two-factor authentication are:

1. Something you know (as a secret password).

2. Something you have (as a secure device with a secret key).

Combining the two factors in the same authentication protocol could increase the security because the intruder would have to break two protections.

Smart card based password authentication is one of the most convenient and commonly used two-factor authentication mechanisms. This technology has been widely deployed in various kinds of authentication applications including remote host login, online banking, access control of restricted vaults, activation of security devices and many more. A smart card based password authentication scheme involves a server *S* and a client A with an identity ID. At first, S securely issues a smart card to A with the smart card being personalized with respect to ID and an initial password. This phase is called the registration phase and is carried out only once for each client. Later on, A can access S in the login and authentication phase, and this phase can be carried out as many times as needed. In this phase, there can be various kinds of passive and active adversaries in the communication channel between A and S. They can modify, remove or insert messages into the channel.

## 2. TWO-FACTOR AUTHENTICATION SCHEMES

In literature, there have been many smart card based password authentication schemes [7, 8, 9, 12, 18, 20, 21, 24] suggested. In Lee *et al.*'s scheme [12], two password based two-factor authentication and key exchange protocols are proposed. The first protocol does not provide pseudo identity and the second protocol provides identity protection. Both protocols require only two message exchanges. These proposed protocols are suitable for low-power devices such as PDAs in public wireless LANs which require mutual authentication, low computation cost, identity protection and less exchanged messages. In Hwang *et al.*'s scheme [8], a secure mutual authentication method is introduced. In Wu and Zhu's scheme [24], a secure authenticated key exchange protocol is presented that achieves fully two-factor authentication and provides forward security of session keys. They have used

user's unique identity to accomplish authentication, instead of using public keys. They used nonces instead of timestamps to avoid the clock synchronization problem. Their scheme allows users to change their password freely without any interaction with the server. They have also given a security proof of their protocol using random-oracle model. In Maharana and Khilar's scheme [31], a smart card based user authentication scheme based on elliptic curve cryptography for large scale hierarchical wireless sensor networks is presented. This scheme combined ECDH (Elliptic curve Diffie–Hellman) and cryptographic hash function to provide authentication as well as a session key for further communication between user and cluster head. Here, feasibility of ECC in context of WSN is demonstrated. It provides mutual authentication between user and base station as well as base station and cluster head. It provides option for dynamic node addition where there is no need to update any information in user smart card for accessing real time data for any addition or replacement of cluster heads in the networks. It also provides a secret session key for further communication between user and the cluster head. This scheme implements merit of using ECC-based mechanism in WSN and enhances the WSN authentication with higher security than other protocols. Das [25] proposed a two-factor user authentication protocol for WSN using only hash function. This protocol avoids many logged in users with the same login id and stolen verifier attacks, which are prominent threats for a password based system if it maintains verifier table at the gateway node or sensor node. In addition, it resists other attacks in WSN except the denial-of-service and node compromise attacks. Also, the efficiency of the proposed protocol is compared with the related ones. Khan and Alghathbar [26] have shown in their scheme that a recently proposed two-factor user authentication scheme in WSN environment is insecure against different kinds of attack and should not be implemented in real applications. They have demonstrated that in Das's scheme [25], there is no provision for users to change or update their passwords, the gateway node bypassing attack is possible, it does not provide mutual authentication between gateway node and sensor node, and it is susceptible to privileged insider attack. To remedy these flaws, they have proposed security patches and improvements which overcome the weak features of the Das's scheme. The presented security improvements can easily be incorporated in the Das's scheme for a more secure and robust two-factor user authentication in WSNs. Nyang *et al.* [28] pointed out that Das's [25] two-factor user authentication protocol is weak against the off-line password guessing attack by insiders and showed that a simple patch that appends secret parameter to the authentication information can eliminate this weakness without sacrificing any efficiency and usability. Also, to protect query responses from wireless sensor nodes to a user, they proposed an efficient method which can be easily implemented using a built-in AES function in sensor nodes. Finally, they gave a guideline for secure implementation of authentication protocols which prevents the outsider who captures a sensor node from mounting password guessing attack and from impersonating the gateway node. Vaidya *et al.* [29] have proposed an improved two-factor user authentication scheme to overcome the security weaknesses of the previous schemes [25, 26] for WSN. Their scheme is resilient to stolen verifier attacks as well as other common types of attacks. They have provided security evaluation and efficiency analysis, which shows that their protocol is more robust and secure than the existing schemes. However, their scheme does not provide session key agreement and mutual authentication between user and sensor node/gateway node. Pu [30] suggested that in addition to the five desirable properties (client authentication, server authentication, server knows no password, freedom of password change and prevention from guessing attack), key compromise impersonation resilience should also be added as one more important security requirement for two-factor smart card based password mutual authentication [21]. It means the adversary should not be able to masquerade any user to access the server's service once if the long-term key of the server is compromised. They provided an attack to illustrate the adversary is able to masquerade any user to access the server's service in their protocol once if the long-term key of the server is compromised. Finally, they have proposed such an improved protocol that eliminates the security weakness existing in Yang *et al.'s* protocol [21] i.e. allowing key compromise impersonation.

## 3. PROBLEM FORMULATION

After reviewing all papers it has been concluded that various two-factor authentication schemes have been proposed in different settings. These schemes resist various security attacks. Security analysis of these schemes will lead to comparison of their efficiency. Some of these schemes do not provide security against denial of service attack, password guessing attack, sensor node compromise attacks. These suffer from user anonymity and increased communication cost. Therefore, an enhanced two-factor authentication scheme is to be proposed that can resist various security attacks as well as provide user anonymity.

## 4. PROPOSED WORK

In the proposed work a two-factor authentication scheme has been provided which will prevent the attacks in network by eliminating the attack races by matching it with knowledge available in the network. Best way to fetch results based on the proposed scheme is to provide secure matching of malicious traffic with knowledgebase available in the backend. But due to delay in matching, pseudonym combo concept is chosen for matching which could be very useful in cutting delay from matching process. The server stores information of register users with pseudonyms and actual ID of users to reveal the anonymity in case of a problem.

The proposed work starts with deployment of enterprise network structure and continues with implementation of traffic on multi interface LAN network. After this process, distributed server structure and a storage area structure has been used. This can store various traces of logs and attack sequences and overall act as database for every process which is helpful in providing encryption process. Header management is the important part of this research as it has managed the size of data required for tracing the knowledge required for detection of malicious traffic. The concept of trace carrying and matching is used by carrying 2 bit information in header for frequent correlated match processed through two-factor authentication at server of any malicious activity.

## 5. SCENARIOS AND SETTINGS

In this work, three existing two-factor authentication schemes from the literature survey have been implemented and then the proposed scheme is implemented. After that the scenarios for security attacks on the proposed scheme have been implemented.

Scenario I: Hwang *et al.*'s scheme [8].

Scenario II: Lee *et al.*'s scheme [12].

Scenario III: Wu and Zhu's scheme [24].

Scenario IV: Proposed two-factor authentication scheme.

Scenario V: Denial of Service Attack in the proposed scheme.

Scenario VI: Man In the Middle Attack in the proposed scheme.

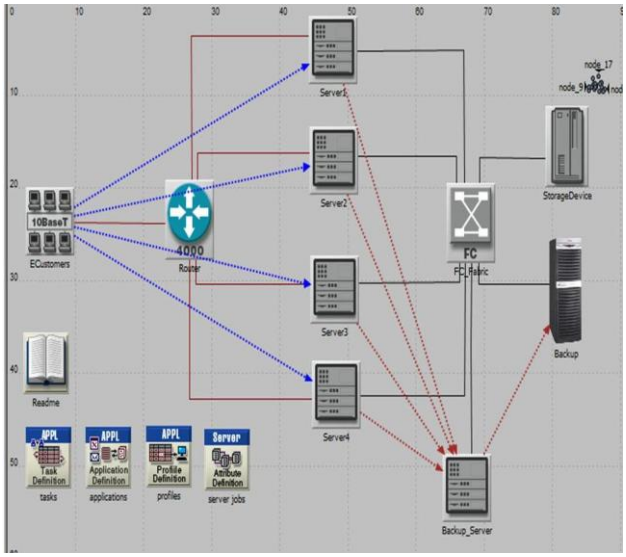


**Figure 1: Scenario I**

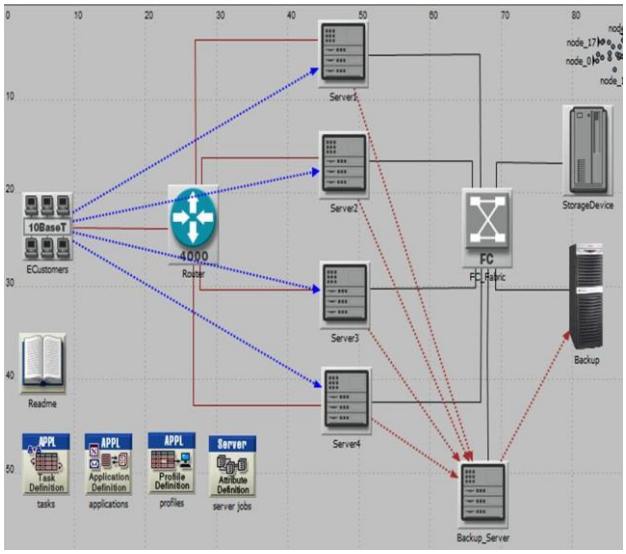


**Figure 2: Scenario II**

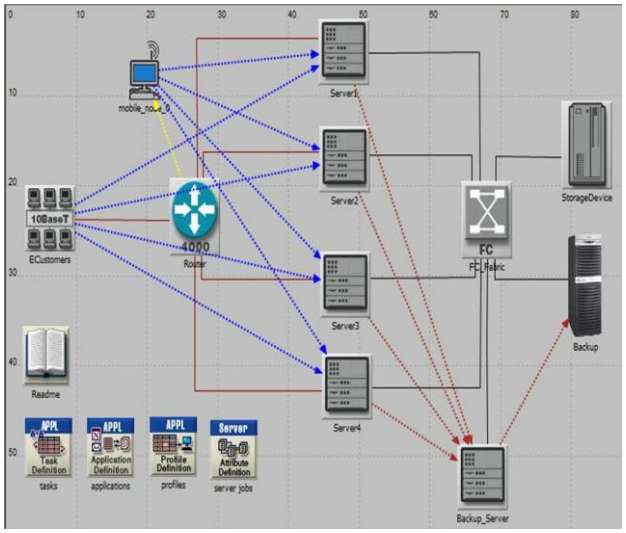


**Figure 3: Scenario III**

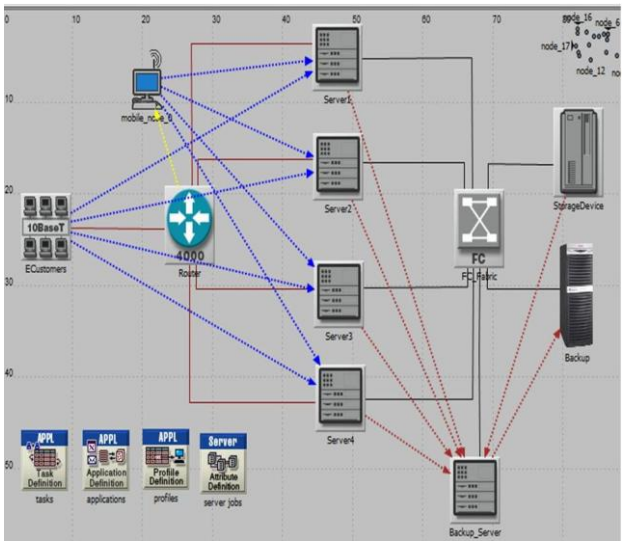


**Figure 4: Scenario IV**

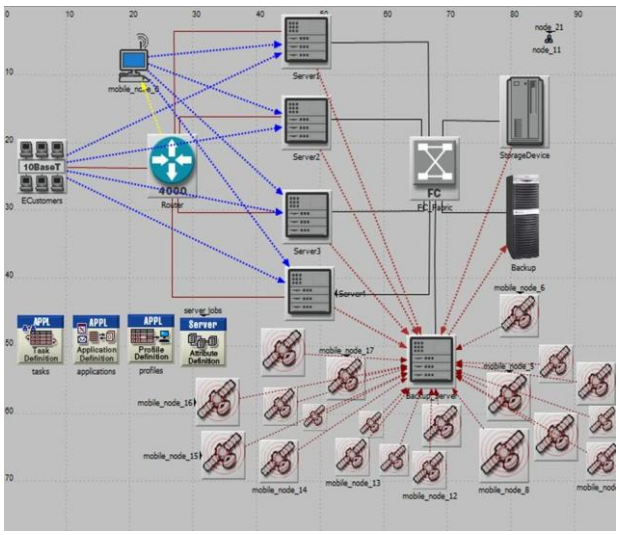


**Figure 5: Scenario V**

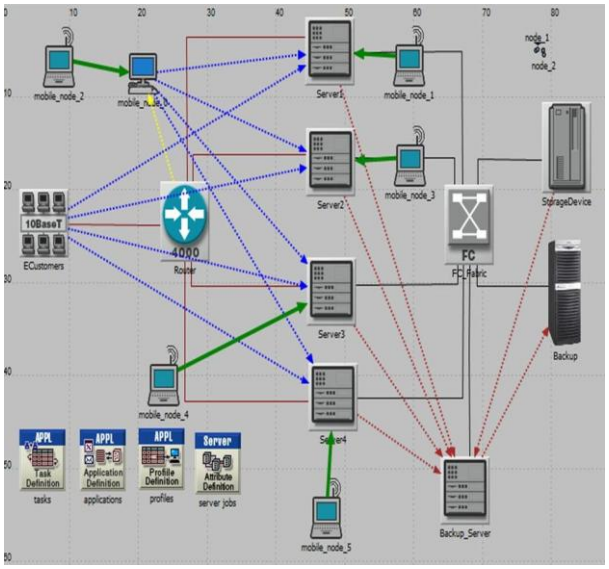


**Figure 6: Scenario VI**

## 6. SIMULATION EVALUATION AND RESULT ANALYSIS

Six graphs are selected after simulating and considering the six scenarios. Results are judged on the basis of response time, CPU utilization and throughput of wireless LAN. First, the average response time, average CPU utilization and wireless LAN throughput have been compared for the various schemes. Then the performance of the proposed scheme with various security attacks is analyzed.

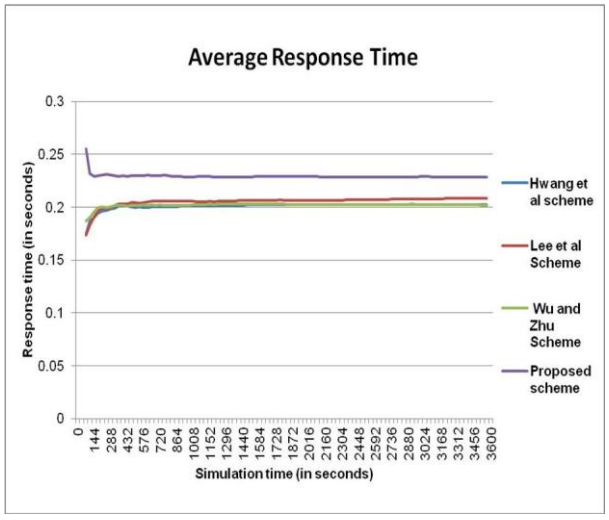


**Figure 7: Average Response Time for implemented schemes**

Figure 7 shows the comparison of average response time of the three existing schemes with the proposed scheme. With Hwang *et al.*'s scheme response time varies from 0.17s to 0.20s. With Lee *et al.*'s scheme it varies from 0.17s to 0.20s. With Wu and Zhu's scheme it varies from 0.18s to 0.20s and with proposed scheme it varies from 0.23s to 0.22s.This analysis shows that for the proposed scheme response time decreases initially but then it becomes stable.

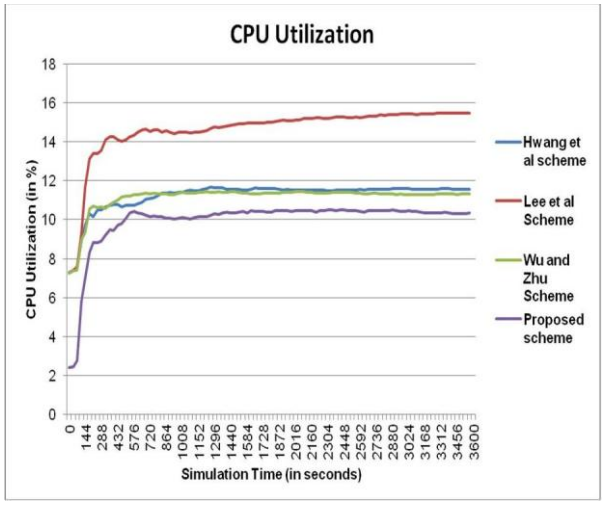


**Figure 8: Average CPU utilization of implemented schemes**

Figure 8 shows average CPU utilization for the three existing schemes and the proposed scheme. It varies from 7.29% to 11.57% with the Hwang *et al.*'s scheme. With Lee *et al.*'s scheme it varies from 7.26% to 15.43%. With Wu and Zhu's scheme it varies from 7.26% to 11.51% and with proposed scheme it varies from 2.42% to 10.50% .This shows that CPU utilization for the proposed scheme increases initially but then it becomes stable and it is better than the other three schemes.

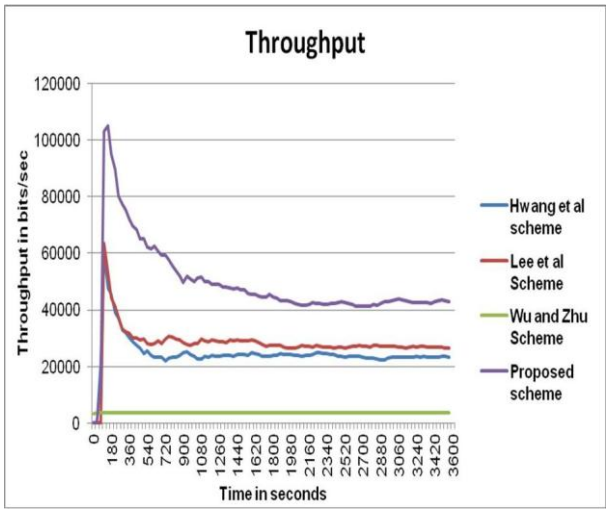


**Figure 9: Comparison of WLAN. Throughput**

Figure 9 shows the comparison of proposed scheme with other schemes in terms of throughput of wireless LAN. Threshold value of throughput for proposed scheme is 105163 bits/sec. After reaching its threshold value, it decreases up to 43031 bits/sec. With Hwang *et al.*'s scheme, it reaches 59701bits/sec and then decreases up to 23388 bits/sec. For Lee *et al.*'s scheme it reaches 63481 bits/sec and decreases up to 26452 bits/sec. For Wu and Zhu's scheme it varies from 3445 bits/sec to 3648 bits/sec. From this it is clear that throughput for the proposed scheme is higher than the other schemes.

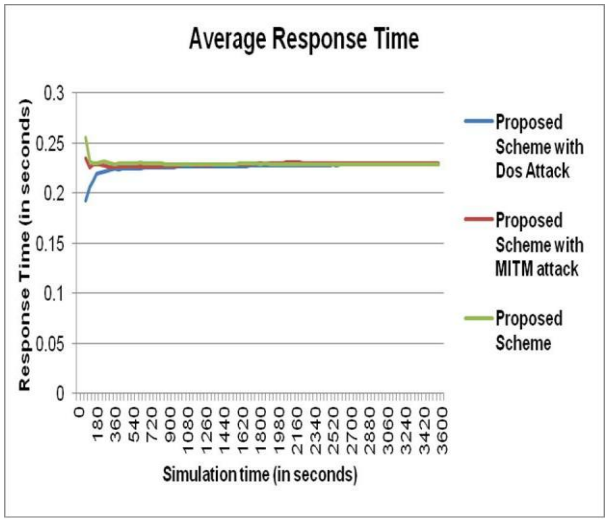


**Figure 10: Effect of security attacks on the average response time of proposed scheme**

Figure 10 shows that the proposed scheme has successfully reduced the effect of denial of service attack and man in the middle attack by retaining the response time for application to its original value 0.22s.

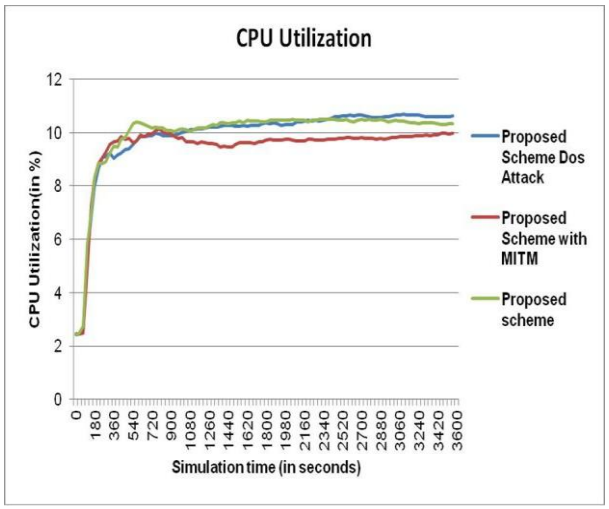


**Figure 11: Effect of security attacks on the average CPU utilization of proposed scheme**

Figure11 shows that in the presence of Denial of service attack, CPU utilization of the proposed scheme initially increases up to 10.67% and then decreases up to 10.61%. In the presence of man in the middle attack, CPU utilization of the proposed scheme initially increases up to 10.14% and then decreases up to 9.95 %.

Figure 12 shows that throughput is increasing initially up to 105163 bits/sec and then descreases up to 43031 bits/sec for proposed scheme. With Denial of service of attack the throughput increases initially up to 92697 bits/sec and then decreases up to 55850 bits/sec. With man-in-the-middle attack, throughput increases initially up to 86196 bits/sec and then decreases up to 34442 bits/sec. The proposed scheme's performance shows that it resists the attacks.

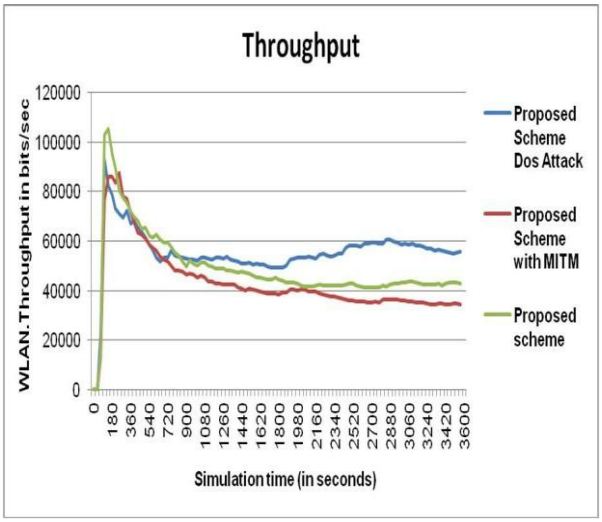


**Figure 12: Effect of security attacks on the WLAN Throughput**

## 7. CONCLUSION

In this paper, the three existing two-factor authentication schemes: Hwang *et al.*'s two-factor authentication scheme; Lee *et al.*'s two-factor authentication scheme; Wu and Zhu's two-factor authentication scheme, have been implemented and compared. Then an enhanced scheme is introduced and after this, the enhanced two-factor authentication scheme is crypt analyzed which can resist various security attacks. The performance analysis shows that average response time of the proposed scheme decreases gradually and then becomes constant. The value of CPU utilization for the proposed scheme is better than the other schemes. Also the wireless LAN throughput is higher in case of proposed scheme. The proposed scheme has successfully reduced the denial of service attack and man in the middle attack by retaining the response time and CPU utilization for application to its original value.

## 8. REFERENCES

[1] Abdalla M., Bellare M. and Rogaway P. "The Oracle Diffie-Hellman Assumptions and an Analysis of DHIES" in Proceedings of the Cryptographer's Track at RSA, pp. 143-158, 2001.

[2] Abdalla M., Chevassut O. and Pointcheval D. "One-Time Verifier-Based Encrypted Key Exchange" in Proceedings of Public Key Cryptography, pp. 47-64, 2005.

[3] Bellare M., Pointcheval D. and Rogaway P. "Authenticated key Exchange Secure Against Dictionary Attacks" in Proceedings of international conference on Theory and application of cryptographic techniques EUROCRYPT, pp. 139-155, 2000.

[4] Bresson E., Chevassut O. and Pointcheval D. "New Security Results on Encrypted Key Exchange" in Proceedings of Public Key Cryptography, pp. 145-158, 2004.

[5] Chien H., Jan J. and Tseng Y. "An Efficient and Practical Solution to Remote Authentication: Smart Card" Computer Journal of Secures, vol. 21, no. 4, pp. 372-375, 2002.

[6] Hankerson D., Menezes A. and Vanstone S. "Guide to Elliptic Curve Cryptography" Springer-Verlag, USA, 2004.

[7] Hwang M. "Cryptanalysis of Remote Login Authentication Scheme" Computer Journal of Communications, vol. 22, no. 8, pp. 742-744, 1999.

[8] Hwang M., Chong S. and Chen T. "DoS- Resistant ID-Based Password Authentication Scheme Using Smart Cards" Computer Journal of Systems and Software, vol. 83, issue 1, pp. 163-172, 2010.

[9] Hwang M., Lee C. and Tang Y. "An Improvement of SPLICE/AS in WIDE Against Guessing Attack" Internet Journal of Information, vol. 12, no. 2, pp. 297-302, 2001.

[10] Koblitz N. "Elliptic Curve Cryptosystem" Computer Journal of Mathematics Computation, vol. 48, no. 3, pp. 203-209, 1987.

[11] Lamport L. "Password Authentication with Insecure Communication" Computer Journal of Communications ACM, vol. 24, no.11, pp. 770-771, 1981.

[12] Lee Y., Kim S. and Won D. "Enhancement of Two-Factor Authenticated Key Exchange Protocols in Public Wireless LANs" Computers and Electrical Engineering, vol. 36, issue 1, pp. 213-223, 2010.

[13] Liao I., Lee C. and Hwang M. "A Password Authentication Scheme over Insecure Networks" Computer Journal of System Science, vol. 72, no. 4, pp. 727-740, 2006.

[14] Mitchell C., Ward M. and Wilson P. "On Key Control in Key Agreement Protocols" Computer Journal of Electronics Letters, vol. 34, no. 3, pp. 980-981, 1998.

[15] Okamoto T. and Pointcheval D. "The Gap- Problems: a New Class of Problems for the Security of Cryptographic Schemes" in Proceedings of Public Key Cryptography, pp. 104-118, 2001.

[16] Pointcheval D. and Zimmer S. "Multi-Factor Authenticated Key Exchange" in Proceedings of Applied Cryptography and Network Security, pp. 277-295, 2008.

[17] Quisquater J. "Side Channel Attacks-Stat" October, http://www.ipa.go.jp/security/enc/CRYPTREC/fy15/doc/1047_Side_Channel _report .pdf, Last Visited 2002.

[18] Scott M. "Cryptanalysis of an Id-Based Password Authentication Scheme Using Smart Cards and Fingerprints" Computer Journal of SIGOPS Operation System Review, vol. 38, no. 2, pp. 73-75, 2004.

[19] Sklavos N., Alexopoulos E. and Koufopavlou O. "Networking Data Integrity: High Speed Architectures and Hardware Implementations" The International Arab Journal of Information Technology, vol. 1, no. 2, pp. 54-59, 2003.

[20] Wang B., Li J. and Tong Z. "Cryptanalysis of an Enhanced Timestamp-Based Password Authentication Scheme" Computer Journal of Secures, vol. 22, no. 7, pp. 643-645, 2003.

[21] Yang G., Wonga D., Wang H. and Deng X. "Two-Factor Mutual Authentication Based on Smart Cards and Passwords" Journal of Computer and System Sciences, vol. 74, no. 7, pp. 1160-1172, 2008.

[22] Yoon E., Ryu E. and Yoo K. "Efficient Remote User Authentication Scheme Based on Generalized Elgamal Signature Scheme" Computer Journal of IEEE Transaction Consumer Electronic, vol. 50, no. 2, pp. 568-570, 2004.

[23] Yoon E. and Yoo K. "New Authentication Scheme Based on a One-Way Hash Function and Diffie-Hellman Key Exchange" in Proceedings of Cryptology and Network Security, China, pp. 147-160, 2005.

[24] Wu S. and Zhu Y. "Improved Two-Factor Authenticated Key Exchange Protocol" The International Arab Journal of Information Technology, vol. 8, no. 4, October 2011.

[25] Das M. L. "Two-Factor User Authentication in Wireless Sensor Networks" IEEE Trans. Wireless Comm., vol. 8, pp. 1086-1090, 2009.

[26] Khan M. K. and Alghathbar K. "Cryptanalysis and Security Improvements of Two-Factor User Authentication in Wireless Sensor Networks" Sensors, vol. 10, no. 3, pp. 2450-2459, 2010.

[27] Juang W. "Efficient password authenticated key agreement using smart card" Computers & Security, vol. 23, pp. 167–73, 2004.

[28] Nyang D. H. and Lee M.K. "Improvement of Das's Two-Factor Authentication Protocol in Wireless Sensor Networks" Cryptology ePrint Archive 2009/631. Online PDF: http://eprint.iacr.org/2009/631.pdf (accessed on 28 February 2010).

[29] Vaidya B., Makrakis D. and Mouftah H. T. "Improved Two-factor User Authentication in Wireless Sensor Networks" Second international workshop on network assurance and security services in ubiquitous environment, 600-606, October 2010.

[30] Pu Q. "An Improved Two-factor Authentication Protocol" Second International Conference on Multimedia and Information Technology, 2010.

[31] Maharana R. and Khilar P. M. "An Improved Authentication Protocol for Hierarchical Wireless Sensor Networks using ECC" International Journal of Computer Applications (0975 – 8887), vol. 67, no. 22, April 2013.