ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 5, Issue 4, April 2018

Preventing Security Attacks Using New Authentication Key Protocol for Wireless Sensor Networks

[1] D J Samatha Naidu, [2] Dr.P,Chitti Babu, [3] A.Roja
[1] Assistant Professor, MCA Department,APGCCS, [2] Principal, APGCCS, [3]MCA Student

Abstract: In research era of wireless sensor networks security related issues are raised online and offline mode packet transmission. Previous progress works are focuses on security attacks either online mode or offline mode only. In Proposed work to prevent security attacks using new authentication key protocol for wireless sensor networks end to end secure communication required. This Proposed new authentication protocol performance study shows that it can be deployed in practice for internet through integrated Wireless Sensor Network, to achieve a security and efficiency.

Index Terms - Introduction, Related Work, new authentication protocol, Performanace Analysis.

1. INTRODUCTION

Random selective secured user authentication key protocol based on the Rabin cryptographic system which has the characteristic of computational asymmetric key exchange. We conduct synopsis based a formal key verification of proposed protocol using Pro-Verify in order to demonstrate that scheme fulfills the required security measurement features. In this paper a comprehensive based heuristic oriented security analysis to show that our protocol is secure than other possible attacks and provides the desired security features.

Motivation work

Random selective secure user authentication protocol scope is fulfills the required security features. This protocol present a inclusive heuristically supports security performance analysis to show that our protocol is secure other possible attacks and provides the desired security features. The results we obtained show that our new protocol is a secure and lightweight solution for authentication and key management for Internet integrated WSNs.

II. EXISTING WORK – LIMITATIONS

In the existing work, various security mechanisms have been proposed to prevent unauthorized access to the sensor data in transit. Li et al. proposed a two phase sign-cryptographic scheme to protect the information flow between a sensor and an entity outside the WSN, which fulfills confidentiality, integrity, authentication, and non-repudiation in one step.[1] However, bilinear pairing is used in the scheme, which makes it unsuitable (because of its high computation and processing overheads) for regular SNs. [2]

Disadvantages

- There is only 2FA Protocol and provides less security.
- Only 32 Bit Hash functions which will give very less security.

III. PROPOSED WORK – ADVANTAGES

In the proposed system, First, we analyze the most recent 3FA protocol and we present its security limitations. Specifically, by comparing with protocol suffers from Type I SSLA (the secret data obtained from the smart card is enough for an adversary to reveal user password) and Type II SSLA (the transcripts of an authentication session are needed for an attacker, in addition to the secret parameters in the user's smart card). Specifically, the user identity and password can be exhaustively guessed in An offline manner along with the secrets stored in the stolen smart card and the intercepted authentication messages. An Issue raised with protocol like KSSTIA if the temporal parameters in an authentication session are disclosed. Furthermore, the protocol is prone to tracking attack and cannot fulfill user intractability.[3]

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 5, Issue 4, April 2018

Second, we present an efficient and secure 3FA protocol based on the Rabin cryptographic system. Other public key-based encryption algorithms such as RSA and ECC, Rabin has the characteristic of computational asymmetric. In this case, the encryption is very efficient while the decryption is relatively heavyweight.[4] This feature is particular well suited for Internet integrated WSN because the mobile device of users is generally resource constrained while the gateway has no such restriction.

Third, conducted a formal verification using Pro Verify to demonstrate that our protocol fulfills the required security features. Furthermore that proposed protocol is capable of active and passive attacks including the security weaknesses revealed in the protocol . Additionally, performance analysis shows that proposed protocol is a solution that can provide authentication and key agreement for Internet integrated WSN, while achieving both security and efficiency.[5]
Advantages
The system implemented using 3FA which provides more security.

IV. PROPOSED WORKING METHODS

a) Localized monitoring
Localized monitoring only generates localized traffic and has been used successfully for node failure detection in static networks. Sensor nodes using Global Positioning System is not suitable, because it is less energy efficient and expensive. It is consumes high energy and not suitable for a network like wireless sensor networks. Our proposed work helps us to prevent security attacks and energy will be less consumption.
b) Location Estimation
By localized monitoring, we can easily identify the failure nodes and the messages can moving out of the transmission range, location estimation is helpful to resolve this ambiguity..
c) Node Collaboration
Through this module, we can improve the decisions which are taken during Location estimation module. Detecting node failures in wireless sensor networks is research challenging because the network topology can be highly dynamic.

Proposed Algorithms

Algorithm
For our analysis we consider three request management strategies: the proposed Performance Gain Prediction algorithm, a Local algorithm that never triggers request redirection and is used as the worst case scenario, and a Threshold-based algorithm that represents a state-of-the-art solution for request management. The Threshold-based algorithm activates redirection on the basis of a local knowledge about the server load. To evaluate the server load metrics, this algorithm relies on the CPU utilization ρsa(t) ,, because it is bounded in the [0,1] interval and is more convenient than process queue length that has no maximum value. For a fair comparison, we apply the DES smoothing techniques also to the CPU utilization to reduce the effect of high variability in samples that could hinder the performance of the Threshold value based algorithm. The each incoming request, the load of the server sais evaluated: if it exceeds a given threshold Thr, the request r is redirected and the corresponding user session is migrated.If the redirection is activated, the remote server is selected through the K-Least Loaded algorithm.[7]

To ensure a fair comparison between the Performance Gain Prediction and the Threshold-based algorithms, we consider that the K-Least Loaded algorithm relies on the same load metric, that is the process queue length, to identify the K=3 servers with the lowest load. We performed some experiments with different values of the K parameter, ranging from 2 to 5, but this does not change the results of the comparison between the redirection algorithms.The condition for request redirection is expressed as:ˆ ρsa(t) > Thr, where the value of Thr = 0.7 is chosen on the basis of preliminary experiments.

Step 1: The public key primitive Rabin cryptosystem is employed to avoid black hole tracking attack.
Step 2: The concept of fuzzy verifier is adopted to achieve local password verification.

Step 3: The timestamp mechanism mitigates session specific temporary information attack. Our new protocol also has 9 phases. SN registration and post-deployment phase which remain unchanged are omitted here.
Biohashing
Rabin cryptosystem
System setup
SN registration
User registration
Login
Authentication
Post-deployment
Identity Update
Password change

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 5, Issue 4, April 2018

Smart card revocation

V. RESULTS

The following software and Hardware requirements can be used to develop this paper.

Hardware Requirements

Processor	: Core2duo
Hard Disk	: 160GB
RAM	:1GB

Software Requirements

Operating System	:Windows XP/or 2007 Linux/Solaris
User Interface	:HTML, CSS
Client-side Scripting	:JavaScript
Programming Language	:Java
API	:JDBC, Servlets , JSP
IDE/Workbench	: My Eclipse 8.6
Database	: Oracle 10g
Server Deployment	:Tomcat 6.x

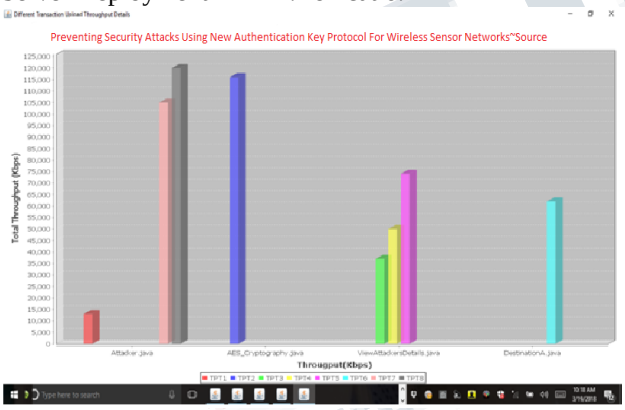

Fig 1: Final analysis report for throughput

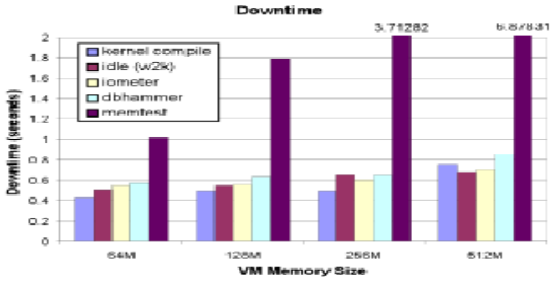

Fig 2a) Total download time 2b)Total migration time

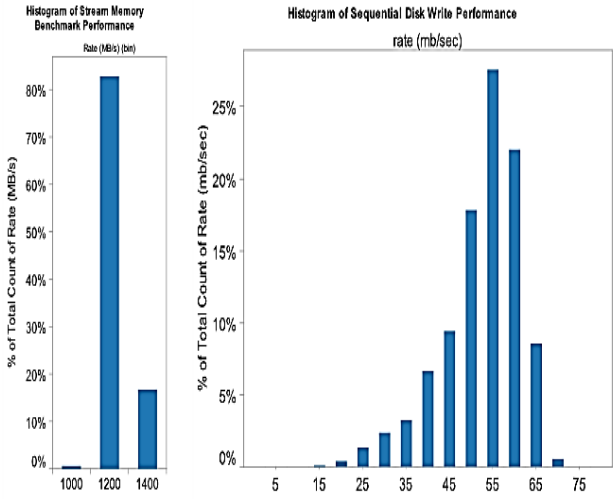

Fig 3 Histogram and benchmark performance.

VI CONCLUSION

Finally, the protocol is horizontal to track show aggression and fails to fulfill user untraceability. Next, we have presented a lightweight and secure three factor authentication protocol based on Rabin cryptosystem. We conducted a formal verification of the proposed protocol by using Pro Verify to demonstrate that it fulfills the required security features. Further our performance analysis , our proposed protocol support all the desired security features in multipath scheduling

REFERENCES

[1] J. Granjal, E. Monteiro, J. S. Silva, "Security in the integration of low power wireless sensor networks with the internet: A survey", Ad Hoc Netw., vol. 24, pp. 264-287, Jan. 2015.

[2] Z. Sheng, S. Yang, Y. Yu, A. Vasilakos, J. McCann, K. Leung, "A survey on the IETF protocol suite for the Internet of Things: Standards challenges and opportunities", IEEE Wireless Commun., vol. 20, no. 6, pp. 91-98, Dec. 2013.

[3] R. Roman and J. Lopez, "Integrating wireless sensor networks and the Internet: A security analysis," Internet Res., vol. 19, no. 2, pp. 246–259, 2015.

[4] J. Astorga, E. Jacob, N. Toledo, et al. "Enhancing secure access to sensor data with user privacy support," Computer Networks, vol. 64, pp. 159179, 2014.

[5] J. Qi, X. Hu, Y. Ma, et al. "A Hybrid Security and Compressive SensingBased Sensor Data Gathering Scheme," IEEE Access 3 (2015): 718-724.

[6] Z. Fu et. al, "Achieving Efficient Cloud Search Services: Multi-keyword Ranked Search over Encrypted Cloud Data Supporting Parallel Computing," IEICE Transactions on Communications, vol. E98-B, no. 1, pp.190-200, 2015.

[7] H. Li, D. Liu, Y. Dai, et al. "Engineering searchable encryption of mobile cloud networks: when QoE meets QoP," IEEE Wireless Communications, vol. 22, no. 4, pp. 74-80, 2015.

[8] S. Kumari, M. K. Khan, M.Atiquzzaman, "User authentication schemes for wireless sensor networks: A review," Ad Hoc Networks, vol. 27, pp. 159-194, 2015.

[9] Q. Jiang, J. Ma, X. Lu, and Y. Tian, "An efficient two-factor user authentication scheme with unlinkability for wireless sensor networks," Peer-to-Peer Netw. Appl., vol. 8, pp. 1070–1081, 2014.

[10] Debiao He, Neeraj Kumar, Naveen Chilamkurti. "A secure temporalcredential-based mutual authentication and key agreement scheme with pseudo identity for wireless sensor networks," Information Sciences, vol. 321, pp. 263-277, 2015..