5. Conclusion

Proposed system will detect Jamming and Replay attack by using minimum energy minimization and furthermore prevention by packet filtering technique. We are decreasing the memory usage for detection of replay attack by using hash procedure. By using hash function the energy usage is amplified and Performance is improved. Also the security is increased by using access control mechanism. Secure protocol is ready to achieve the goals of considerably less energy consumption and higher security than previous works. This helps to use the proposed implementation on any operating system. For Future work, we can find the actual source of attack from where the replay and jamming attack is happening.

6. Acknowledgment

We are thankful to the authorities of Savitribai Phule pune University, Pune for their constant guidelines . We also thankful to my guide & college authorities for providing constant guidelines and support. Finally, we would like to extend a heartfelt gratitude to friends and family members.

References

[1] Yao-Tung Tsou, Chun-Shien Lu, Member, IEEE, and Sy-Yen Kuo, Fellow, IEEE, "MoteSec-Aware: A Practical Secure Mechanism for- Wireless Sensor Networks" IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS, VOL. 12, NO. 6, JUNE 2013.
[2] Dalit NaorMoniNaor Jeff Lotspiech, "Revocation and Tracing Schemes for Stateless Receivers".
[3] Chia-Mu Yu, Chun-ShienLu,andSy-Yen Kuo,"A Constrained Function Based Message Authentication Scheme for Sensor Networks" IEEE Communications Society.
[4] M. Luk, G. Mezzour, A. Perrig, and V. Gligor, 'MiniSec: a secure sensor network communication architecture,' in Proc. 2007 International Conference on Information Processing in Sensor Networks, pp. 479488.
[5] Chris Karlof, Naveen Sastry, David Wagner, "TinySec: A Link Layer Security Architecture for Wireless Sensor Networks".
[6] Kun Sun, An Liu, "Securing Network Access in Wireless Sensor Networks" the Department of Homeland Security under grant NBCHC080061.
[7] Madhumita Panda, "Security Threats at Each Layer of Wireless Sensor Networks" Volume 3, Issue 11, November 2013 ISSN: 2277 128X International Journal of Advanced Research in Computer Science and Software Engineering.
[8] SAURABH GANERIWAL, "Secure Time Synchronization in Sensor Networks" ACM Transactions on Information and Systems Security, Vol.11, No. 4, Article 23, Pub. date: July 2008.
[9] Adrian Perrig, Robert Szewczyk, Victor Wen, David Culler, J. D. Tygar, "SPINS: Security Protocols for Sensor Networks" In Proceedings of the 7th Annual International Conference on Mobile Computing and Networks (MOBICOM), July 2001, pp. 189-199
[10] Jin Li, Xiaofeng Chen, Mingqiang Li, Jingwei Li, Patrick P.C. Lee, and Wenjing Lou, "Secure Deduplication with Efficient and Reliable Convergent Key Management" IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, VOL. 25, NO. 6, JUNE 2014.
[11] A. R. Uttarkar, H. A. Hingoliwala, "Secure System Practices and Data Access Management in Wireless Sensor Network" International Journal of Computer Applications (0975 8887) Volume 91 No.11, April 2014.
[12] DeveshJinwala*1, Dhiren Patel2 and Kankar Dasgupta, "FlexiSec: A Configurable Link Layer Security Architecture for Wireless Sensor Networks" Journal of Information Assurance and Security 4 (2009) 582- 603