International Journal of Management, IT & Engineering
Vol. 11 Issue 3, March 2021,
ISSN: 2249-0558 Impact Factor: 7.119
Journal Homepage: http://www.ijmra.us, Email: editorijmie@gmail.com Double-Blind Peer Reviewed Refereed
Open Access International Journal - Included in the International Serial Directories Indexed & Listed at: Ulrich's Periodicals Directory ©, U.S.A., Open J-Gate as well as in Cabell's Directories of Publishing Opportunities, U.S.A

GROUP KEY MANAGEMENT FOR SECURE MULTICASTING IN INTERNET OF THINGS (IOT) BY USING SECRET SHARING TECHNIQUES

Anju Bala[1], Dr. Prasadu Peddi[2]

[1]Research Scholar, Department of Computer Science, Shri Jagdishprasad Jhabarmal Tibrewala University, Jhunjhunu, Rajasthan
[2]Assistant Professor, Department of Computer Science, Shri Jagdishprasad Jhabarmal Tibrewala University, Jhunjhunu, Rajasthan
[1]anju.godara009@gmail.com;[2]peddiprasd37@ymail.com

Abstract

Internet of Things (IoT) is tied in with connecting actual items to the worldwide network (internet) in which information detected by these articles become accessible and distantly open. Group communication discovered to be more productive in utilizing assets than pairwise communication. Group key establishment is vital for secure the communication of the multicast group and give message secrecy, credibility, and integrity. Traditional Secret Sharing schemes use polynomials for generating/reconstructing the shares of the secret S which is considered computationally substantial. AVISPA is a software tool that is generally used to naturally approve the security of internet protocols and applications. We can conclude that the security analysis and the performance evaluation comparison between the proposed scheme and other IoT group key establishment schemes showed that our scheme accomplishes better security and use the network and gadgets assets effectively.

Keywords:internet of things, secure, multicasting, secret, sharing, techniques, etc**.**

1.INTRODUCTION

Internet of Things (IoT) is tied in with connecting actual items to the worldwide network (internet) in which information detected by these articles become accessible and distantly open. IoT opens new open doors in a few applications domains like keen home, savvy urban areas, medical care monitoring, natural monitoring and shrewd horticulture, an illustration of brilliant agribusiness is the keen watering framework, it is applied in homes, gardens and big farms. The brilliant watering framework is significant explicitly in regions with scant water assets. Key management is one of the fundamental security prerequisites to secure communication and to guarantee secrecy, confirmation, and integrity of messages

traded in a framework. Group communication discovered to be more productive in utilizing assets than pairwise communication. Nonetheless, the lopsidedness capacities of the IoT asset constrained gadgets and the weighty cryptographic elements of the existing customary group key establishment protocols elevate scientists to create elective arrangements that depend on lightweight security natives to give start to finish security

And to ensure the information stream in IoT climate group key establishment is vital for secure the communication of the multicast group and give message secrecy, credibility, and integrity. IoT depends generally on sensors which they don't have an amazing computational ability, memory limit, and additionally absence of reliable energy, be that as it may, the security arrangements accommodated such gadgets ought to be lightweight and strong.

1.1 Key Establishment for Secure Multicasting in IoT Enabled Wireless Sensor Networks

Wireless Sensor Network (WSN) is a key building square of Internet of Things (IoT). Sensors are asset constrained with restricted memory, battery force and calculation abilities. Therefore, it is more and effective to pass on multicast messages to a group of gadgets instead of sending energy consuming unicast messages to individual gadgets in different duplicates. Secure group key establishment is a significant trait to give integrity, validation, and secrecy for message transmissions in these multicast groups. In addition, group key establishment protocols need to help gadget and network attributes in IoT-enabled WSNs like asset constraints, adaptability, and dynamic group formation. This paper explains two group key establishment protocols for secure multicasting in IoT enabled WSN applications. The relevance of the protocols is portrayed in the light of IoT attributes alongside performance and security examination. It is defended that the arrangements proposed have better performance attributes and relieve the existing security weaknesses of the arrangements given in the cutting edge.

2. LITERATURE REVIEW

Basu, Subho and Somanath, Tripathy (2019) with the coming of Internet of Things (IoT) and the wide number of utilizations that it is being applied on; in the long run it will outperform the current size of the Internet. Be that as it may, with this number of gadgets serving such countless applications and being reachable distantly absurd, they become

similarly inclined towards attacks and weaknesses. Consequently, productive and secure systems custom-made to such convenient gadgets are to be planned. In particular the protocols running on these gadgets need to fulfill the essential security necessities while consuming minimum assets as far as memory, bandwidth and force. Additionally as these gadgets will be in millions there is an increasing need to plan multicast security systems as large numbers of the applications require it. Till date there has been restricted commitment towards multicast security with approaches made mainly dependent on extending the DTLS protocol, which certainly has various disadvantages.

Basu, Subho and Somanath, Tripathy (2018) latest thing is being reached out from the customary Internet to the little, modest, and low-power Internet of Things (IoT) in which the items are being outfitted with a gadget having calculation and communication capacities. Therefore, every one of these articles can be associated with the Internet and have the capacity to convey among one another. This association infrastructure among the articles would confront various kinds of malicious attacks. Consequently securing these articles is an essential objective. There are a great deal of security instruments accessible today, however a large portion of them are very weighty regarding calculation and communication. As the IoT objects have exceptionally restricted assets and for the most part run on battery power, it is hard to install intensive calculations on this asset constrained gadgets. Datagram Transport Layer Security (DTLS) protocol has been standardized to work in attachment with the CoAP protocol to give security.

Porambage, Pawani and Braeken, A and Schmitt, Corinna and Gurtov, Andrei and Ylianttila, Mika and Stiller, Burkhard (2015) Wireless Sensor Network (WSN) is a prominent central innovation of the Internet of Things (IoT). Instead of gadget to-gadget communications, group communications in the form of broadcasting and multicasting incur productive message conveyances among asset constrained sensor hubs in IoT-enabled WSNs. Secure and effective key management is important to ensure the genuineness, integrity, and classification of multicast messages. This paper creates two group key establishment protocols for secure multicast communications among asset constrained gadgets in IoT. Significant sending conditions and prerequisites of every protocol are portrayed as far as the particular IoT application situations. Besides, the appropriateness of the two protocols is investigated and advocated by a far reaching examination of performance, adaptability, and security of those protocols proposed.

Lee, Chia-Yin and Wang, Zhi-Hui and Harn, Lein and Chang, Chih-Hsiang (2011) group key establishment is a significant instrument to build a typical meeting key for group communications. Ordinary group key establishment protocols utilize an on-line believed key generation center (KGC) to move the group key for every member in every meeting. In any case, this methodology necessitates that a believed worker be set up, and it incurs communication overhead expenses. In this article, we address some security issues and downsides related with existing group key establishment protocols. In addition, we utilize the idea of secret sharing plan to propose a secure key exchange protocol to prohibit impersonators from accessing the group communication. Our protocol can oppose likely attacks and additionally decrease the overhead of framework execution. Likewise, examinations of the security investigation and usefulness of our proposed protocol for certain new protocols are included in this article.

3.OBJECTIVES

- To study Secure Multicasting in IoT Enabled Wireless Sensor Networks.
- To analyze aboutSecurity analysis and Formal Security Verification.

4.RESEARCH METHODOLOGY

4.1 Techniques used

- **Secret Sharing Technique:** Traditional Secret Sharing schemes use polynomials for generating/reconstructing the shares of the secret S which is considered computationally substantial. Nonetheless, Ramp secret sharing scheme attempted to upgrade the share size of Shamir and he accomplished better result instead of share size =|S| in Ramp secret sharing it gets 1\m, where m is the quantity of blocks in the secret S. The XOR network coding, accomplishes a preferable performance over Ramp and Shamir secret sharing schemes by avoiding the polynomials yet unfortunately the tradeoff between upgraded performance and the share size happens as the share size increased in the Xor network coding schemes as it costs (|S|/m + m) instead of |S|/m in Ramp scheme.

- **Slepian-Wolf Secret Sharing Scheme (SW-SSS):** Initially, Slepian-Wolf coding (SWC) was found by David Slepian and Jack Wolf it is a strategy utilized for information compression of theoretically coding two lossless packed corresponded sources. As of late in 2017 based on SWC, Slepian-Wolf Secret Sharing Scheme SW-SSS was proposed as a proficient secret sharing technique. SW-SSS is distinguished from other secret sharing techniques by its advanced share size and the utilization of Xor operation achieving little stockpiling and quick computation which makes it appropriate for a constrained network like IoT.

4.2 Software tool

- **AVISPA Software:** AVISPA (Automated Validation of Internet Security Protocols and Applications) is a software tool that is generally used to naturally approve the security of internet protocols and applications. The tool carries out the Dolev-Yao intruder model, which can listen in, intercept messages, insert sham information, or adjust traffic passing through. The tool has four back-closes for programmed analysis of protocols security which are integrated to HLPSL.

- **HLPSL Specification of the Proposed Protocol:** The protocol is modeled by three members, in particular, the gateway the sensors, and the intermediary. They are addressed as GWN, Nj, and P individually. The implementation of every player is modeled in the fundamental job. HLPSL is an expressive language for modeling communication and security protocols. It is a job based language in which every member (agent) in the protocol is addressed by a job. Jobs are of two sort's fundamental jobs where each agent’s factors are announced using the (Transition) section.

5. RESULT AND DISCUSSION

5.1 Security analysis and Performance evaluation

The evaluation is conducted by two unique techniques. The principal technique demonstrates the high security of the protocol through theoretical security analysis. The second technique is through formal evaluation using AVISPA security analyzing tool. Additionally, performance evaluation is conducted in term computation, communication, energy, and capacity costs consumed by the constrained-gadgets.

- **Performance Evaluations:**

With The Existing IoT Key Establishment Protocols We have conducted a performance evaluation comparison with a portion of the existing key establishment protocols in IoT we present beneath various computation, communication and capacity costs for establishing the session key at the constrained nodes.

  - **Computation Cost:** We have utilized hash functions and Xor operation to accomplish a lightweight computation. Comparing to hashing and xoring operations, ECC point operations (i.e., point addition and multiplication) are considered the most costly calculations. In the proposed scheme gateway and the intermediary are asset rich nodes the absolute computation cost is $2T_h\oplus$ and 16 $T_h\oplus$ +O (m^2) individually.

5.2 Formal Security Verification

To help the result of the theoretical security analysis we carried out our proposed protocol using AVISPA security analyzer tool. AVISPA (Automated Validation of Internet Security Protocols and Applications) is a strong simulation engine for automated security analysis of cryptographic protocols. It is utilized to confirm the security ascribes of protocols and applications. AVISPA utilizes High-Level Protocol Specification Language (HLPSL).

  - **Simulation Result:**

We have utilized the back-closes the on-the-fly Model-Checker (OFMC) and the CL-AtSe (Constraint-Logic-based Attack Searcher). OFMC assembles the infinite tree defined by the protocol analysis issue in a demand-driven way, for example on-the-fly, thus the name of the back-end. It utilizes various representative techniques to address the state-space. CL-AtSe gives a translation from any security protocol specification composed as a transition relation in an intermediate format (IF) into a bunch of constraints, which are successfully used to find security shortcomings of the planned protocol. The result of the proposed protocol as demonstrated for both back-closes in figure 1 and figure 2 is SAFE indicating that the protocol is secure from various kinds of attacks.

Figure 1: Simulation Output result of the proposed protocol using CL-Atse

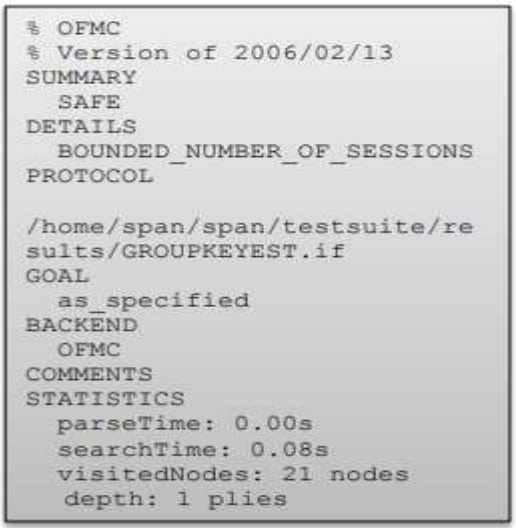

Figure 2: Simulation Output result of the proposed protocol using OFMC

6.CONCLUSION

We can conclude that a Group Key Establishment for secure multicast communication for the IoT environment was proposed. The scheme have utilized the Slepian-wolf secret sharing scheme, hash function and Xor computation to ensure the key confidentiality, integrity, newness, and authenticity. Additionally, the scheme was formally carried out using the AVISPA security analyzer tool the result showed the protocol is SAFE. As a result, the security analysis and the performance evaluation comparison between the

proposed scheme and other IoT group key establishment schemes showed that our scheme accomplishes better security and use the network and gadgets assets effectively.

REFERENCES

1. Basu, Subho & Somanath, Tripathy. (2019). Secure Multicast Communication Techniques for IoT: Technology, Communications and Computing. 10.1007/978-3-030-02807-7_3.

2. Basu, Subho & Somanath, Tripathy. (2018). Securing Multicast Group Communication in IoT-Enabled Systems. IETE Technical Review. 36. 1-11. 10.1080/02564602.2017.1407681.

3. Porambage, Pawani & Braeken, An & Schmitt, Corinna & Gurtov, Andrei & Ylianttila, Mika & Stiller, Burkhard. (2015). Group Key Establishment for Secure Multicasting in IoT Enabled Wireless Sensor Networks. 10.1109/LCN.2015.7366358.

4. Lee, Chia-Yin & Wang, Zhi-Hui & Harn, Lein & Chang, Chih-Hsiang. (2011). Secure Key Transfer Protocol Based on Secret Sharing for Group Communications. IEICE Transactions. 94-D. 2069-2076. 10.1587/transinf.E94.D.2069.

5. Ammar, Mahmoud, Giovanni Russello, and Bruno Crispo. "Internet of Things: A survey on the security of IoT frameworks." Journal of Information Security and Applications38 (2018): 8-27.

6. Wu, Miao, et al. "Research on the architecture of Internet of Things." Advanced Computer Theory and Engineering (ICACTE), 2010 3rd International Conference on. Vol. 5. IEEE, 2010.

7. Lin, Jie, et al. "A survey on internet of things: Architecture, enabling technologies, security and privacy, and applications." IEEE Internet of Things Journal 4.5 (2017): 1125-1142.

8. Agrawal, Shashank, and Dario Vieira. "A survey on Internet of Things." Abakós 1.2 (2013): 78-95.

9. Van Kranenburg, Rob, et al. "The internet of things." Proc. of the First Berlin Symposium on Internet and Society. 2011.

10. Ma, Jianguo. "Internet-of-Things: Technology evolution and challenges." Microwave Symposium (IMS), 2014 IEEE MTT-S International. IEEE, 2014.

11. Fernandes, Earlence, Jaeyeon Jung, and Atul Prakash. "Security analysis of emerging smart home applications." 2016 IEEE Symposium on Security and Privacy (SP). IEEE, 2016.