Securing Internet of Things Applications Using Key Management

Subjects: Computer Science, Cybernetics

Contributor: Antony Taurshia, Jaspher W. Kathrine, J. Andrew, Jennifer Eunice R

The Internet of Things (IoT) emerged when everyday objects began connecting to the Internet and interacting with each other autonomously without human intervention. IoT devices follow the IEEE 802.15.4 standard to enable network connectivity for resource-constrained devices using short-range, lightweight communication protocols.

Keywords: Internet of Things ; key management ; group management ; security

1. Introduction

The Internet of Things (IoT) emerged when everyday objects began connecting to the Internet and interacting with each other autonomously without human intervention. IoT devices follow the IEEE 802.15.4 standard [1] to enable network connectivity for resource-constrained devices using short-range, lightweight communication protocols [1]. Due to the limited availability of device resources in addition to the bandwidth problem, the IoT ecosystem prefers multicast communication instead of unicast messages to send updates and patch-ups [2][3]. To send multicast messages securely, a common secret key need to be shared between the devices in the multicast group. To efficiently distribute the keys to all group devices, a vast amount of group key management techniques have been proposed in the literature. Group key management enables the group to operate with integrity and confidentiality [4]. There are three methods for managing group keys. The Key Management Server (KMS), a trustworthy third party, is utilized for key distribution in the centralized key management technique [5][6]. In decentralized key management, both the server and group member devices contribute to key management [7][8][9]. In distributed key management, there is no centralized trust, but every member participates in key management [10][11][12][13]. Among all three methods, centralized key management offers less communication and computation overhead on the member devices with simpler functions. Hence, the proposed work focuses on centralized key management techniques, considering them to be most suitable for resource-constrained IoT devices. Centralized key management relies on a dependable third-party server for key management and key distribution. The proposed group management server uses an SDN controller to obtain centralized control over the heterogeneous network. The controller provides opinions on whether to forward network traffic, while the routers just obey the controller [14]. The advantages of SDN in comparison with traditional networks [15][16][17] are,

- Easy patching and upgradation
- Knowledge of the sleep/wake cycle of IoT devices
- Supports security services by routing traffic through virtualized service functions known as Virtual Service Functions (VSF)

The distribution of a common group key or key materials needed for group key generation occurs during the rekeying procedure. Rekeying ensures the group's confidentiality by putting forward and backward secrecy into action. When a group member leaves, the departing member should not have any access to any key materials that could be used to access any unapproved group data after the member exit event. This is termed forward secrecy. Similarly, when a new member enters an existing group, the joining member ought not to receive any key materials to obtain any unauthorized group data preceding the member join event. This is termed backward secrecy. A collusion attack is when two or more members join to obtain key material to access the group's data that are unauthorized for the colluding members. An efficient key management technique should ensure both forward secrecy and backward secrecy, as well as resistance to collusion attacks. Chinese Remainder Theorem (CRT)-based methods [18] offer the lowest communication costs out of all the centralized group key management techniques that have been proposed in the literature. However, because of its limited scalability, the method cannot be applied to dynamic groups.

2. SDN-Centered Security for IoT

An architecture for furnishing network security services like an internet content filtering system, firewall, Intrusion Detection System (IDS), Intrusion Prevention System (IPS), and packet inspection using SDN is proposed. The network traffic can be routed through the services based on the needs of the user. The use of SDN for IoT networks to mitigate attacks by limiting the rate of suspicious traffic flow is proposed in [19]. An SDN-based framework for designing cyber resilience for the Industrial IoT (IIoT) is proposed in [20]. The ontology is designed to create pre-programmed failover paths that become activated in the event of failure. This maintains the equilibrium resilience of the IIoT network for effective failure recovery. A similar SDN-based ontology design for cyber resilience in smart manufacturing applications is proposed in [21]. To implement incident response in the IIoT, the use of SDN is proposed in [22] due to its dynamic routing policies. The preconfigured incident–response policy is enforced using SDN in the event of an attack. Invariant-based anomaly detection using SDN for IIoT is proposed in [23]. Invariant is a property of the IIoT network that remains the same in any situation. A change in this property is identified as an anomaly by adding the invariant algorithm to the SDN-controlled switches. An Intrusion Detection and Prevention System (IDPS) is proposed in [24] that exploits SDN and a Genetic Algorithm (GA) to extract features for effective intrusion detection in IoT applications. Advanced reservation-based access control using SDN is proposed in [25]. The advanced reservation of bandwidth for a certain period is employed using SDN. SDN extends the reservation from border routers to the end devices with tokens for authorization. Another SDN-based architecture for smart home networks is proposed in [26]. With SDN, all smart home devices are connected via a gateway. KNOT and Orchestrator are used with the aid of SDN to detect Advanced Persistent Threats and saturation attacks and mitigate them effectively. HanGaurd SDN-based fine-grained protection for a smart home from malicious apps running on authorized devices like a smartphone is proposed in [27]. An SDN-based firewall called FORTRESS is proposed in [28]. The stateful flow data are obtained from the data plane, and the Mealy machine is exploited to perform state table updations based on the routing decision made. An SDN-centered defense mechanism for IoT networks is proposed in [29]. The IoT devices are classified as easily patchable or non-patchable, vulnerable or hard-to-exploit, and a proactive defense mechanism is provided by changing the attack surface in case the device is vulnerable and non-patchable. The features of SDN are exploited to provide a honeypot as a service by steering the traffic through Virtualized Functions (VF) as proposed in [30]. The honeypot acts as a proactive as well as a reactive defense mechanism against attacks. The honeypots are virtualized and provided as a service using SDN. SDN for effective intrusion detection as well as for mitigation of attacks like Distributed Denial of Service (DDoS) in the habitat of the IoT is proposed in [31][32]. DDoS detection system that exploits the convenience of SDN using machine learning techniques is proposed in [33]. The proposed work uses an adaptive multilayered feed-forwarding scheme that uses different algorithms in five layers. The third layer computes the live, real-time network traffic for DDoS attack detection, and SDN mitigates the attacks using Open Flow switches.

3. Group Key Management Techniques

SKDC follows a very simple approach, where all the existing participants of the group share an individual secret key with the KMS. When there is a change in the number of group members, the new group key is handed out by KMS to existing participants of the group individually, encrypted using the shared secret key, in sequential order. Hence, the communication cost is linear, which is highly inefficient for large dynamic groups. The group Diffie–Hellman (DH) proposed in [34] uses asymmetric encryption for key distribution, with higher computation overhead. Logical Key Hierarchy (LKH) [35] is a familiar centralized, hierarchy-based key management approach for dynamic groups. LKH uses a balanced binary tree-based data structure with member devices' keys as leaf nodes. The root node contains the group key. The intermediate nodes along the path of the member devices to the root hold the key encryption keys with which the devices can obtain the group key. The overall overhead of the approach is 2 log n.

Yet another centralized, hierarchy-based key management approach for groups is the OFT, which reduces the communication cost to log n. Hence, the approach reduces bandwidth consumption considerably. The approach is similar to LKH, with the member device's individual keys as leaf nodes. The root key is the group key. The intermediate nodes hold the key-encryption key, which is calculated using a one-way and mixing function on the child node's keys. However, the approach fails to provide collusion resistance where two expelled members collide and can gain access to unauthorized group data. Several advancements to the OFT-based approach are proposed [36][37] to enhance the collusion resistance property, but in turn, the advancements increase the overall overhead. To impart collusion resistance in OFT, two more approaches are proposed in [38]; both approaches successfully impart collusion resistance with the same communication cost as OFT but with higher computation costs.

A centralized key management approach for the group that uses Diffie-Hellman for generating the key-encryption key is proposed in [39]. The group key can be decrypted using the key-encryption key. However, the use of public key

cryptography increases the computation cost greatly. Moreover, without authentication, the use of Diffie-Hellman is liable to man-in-the-middle attack. A lightweight key management approach for groups formed in IoT applications is proposed in. The approach uses a hybrid technique with a combination of CRT and LKH. The intermediate node keys are calculated by hashing the device's ID. Although the ID of a device is unique, tracking the ID of the device is simple for malicious users to perform forgery-based attacks. Group key management using the Chinese Reminder Theorem (CRT) is proposed in. The approach is efficient, with the least communication cost of a single broadcast. When the group size exceeds the preset n value, the individual keys for the entire group must be renewed. A blockchain-based solution for key management in groups for autonomous aerial vehicles has earlier been proposed. The approach uses LKH along with blockchain for group key updations and reduces delay. The approach also assures forward and backward secrecy. However, the use of blockchain in a resource-constrained environment would be a problem. Another lightweight asymmetric group key management approach for VANETS is proposed in [40]. The approach uses a combination of CRT and asymmetric cryptography in contrast to the traditional symmetric group key management techniques. The scheme is comparatively scalable and has minimal computation overhead compared to its predecessor, CRT-based group key management techniques for VANETS. Still, the approach cannot use variable key sizes since the key sizes are chosen based on constraints. Further, a collusion-resistant approach to group key management is proposed in [41], which makes use of tokens to avoid collusions. The approach distributes group keys with a single broadcast with minimal communication load. Still, the storage overhead is high as the devices store the tokens belonging to a device's cognate nodes. A novel protocol, GKMP, for key management in groups, is proposed in [42] to avoid collusion attacks during file sharing in the cloud. The scheme uses a group key generated by participants and not by a centralized cloud server, adding security in terms of file sharing. But the scheme uses RSA for key generation, which is expensive for IoT devices. Yet another communication-aware key management protocol for IoT networks is proposed in [43]. The scheme uses hyperelliptic curve cryptography for authentication along with bilateral generalization in a homogeneous short integer-based solution for effective key management in IoT groups. The scheme has lower computational time compared to its previous similar schemes; still, public key cryptography-based schemes increase the complexity and device overload in IoT networks.

When evaluated in terms of computation, communication, storage load, scalability, and secrecy, the existing techniques in the literature attain efficiency in one parameter with a trade-off in other parameters. OFT reduces the communication cost but does not ensure secrecy. CRT reduces the overall computation, communication, and storage costs but lacks scalability.

References

1. Farash, M.S.; Turkanović, M.; Kumari, S.; Hölbl, M. An efficient user authentication and key agreement scheme for heterogeneous wireless sensor network tailored for the Internet of Things environment. Ad Hoc Netw. 2016, 36, 152–176.
2. Heo, G.; Chae, K.; Doh, I. Hierarchical Blockchain-based Group and Group Key Management Scheme Exploiting Unmanned Aerial Vehicles for Urban Computing. IEEE Access 2022, 10, 27990–28003.
3. Nikbakht Bideh, P. LMGROUP: A Lightweight Multicast Group Key Management for IoT Networks. In International Conference on Information Security Practice and Experience; Springer: Cham, Switzerland, 2022; pp. 213–230.
4. Sakarindr, P.; Ansari, N. Survey of security services on group communications. IET Inf. Secur. 2010, 4, 258–272.
5. Xu, J.; Li, L.; Lu, S.; Yin, H. A novel batch-based LKH tree balanced algorithm for group key management. Sci. China Inf. Sci. 2017, 60, 108301.
6. Kung, Y.-H.; Hsiao, H.-C. GroupIt: Lightweight Group Key Management for Dynamic IoT Environments. IEEE Internet Things J. 2018, 5, 5155–5165.
7. Kim, Y.; Perrig, A.; Tsudik, G. Tree-based group key agreement. ACM Trans. Inf. Syst. Secur. 2004, 7, 60–96.
8. Zhou, W.; Xu, Y.; Wang, G. Distributed Group Key Management Using Multilinear Forms for Multi-privileged Group Communications. In Proceedings of the 2013 12th IEEE International Conference on Trust, Security and Privacy in Computing and Communications, Melbourne, VIC, Australia, 16–18 July 2013.
9. Sepulveda, J.; Flórez, D.; Immler, V.; Gogniat, G.; Sigl, G. Efficient security zones implementation through hierarchical group key management at NoC-based MPSoCs. Microprocess. Microsyst. 2017, 50, 164–174.
10. Ali, S.; Rauf, A.; Islam, N.; Farman, H.; Jan, B.; Khan, M.; Ahmad, A. SGKMP: A scalable group key management protocol. Sustain. Cities Soc. 2018, 39, 37–42.
11. De Salve, A.; Di Pietro, R.; Mori, P.; Ricci, L. Logical key hierarchy for groups management in Distributed Online Social Network. In Proceedings of the 2016 IEEE Symposium on Computers and Communication (ISCC), Messina, Italy, 27–

30 June 2016; pp. 710–717.

12. Inoue, D.; Kuroda, M. FDLKH: Fully decentralized key management scheme on logical key hierarchy. In Applied Cryptography and Network Security; Springer: Berlin/Heidelberg, Germany, 2004; Volume 3089, pp. 339–354.
13. Wu, Q.; Qin, B.; Zhang, L.; Domingo-Ferrer, J.; Farras, O.; Manjon, J.A. Contributory broadcast encryption with efficient encryption and short ciphertexts. IEEE Trans. Comput. 2016, 65, 466–479.
14. Der Chou, L.; Tseng, C.-W.; Huang, Y.-K.; Chen, K.-C.; Ou, T.-F.; Yen, C.-K. A Security Service on-demand Architecture in SDN. In Proceedings of the 2016 International Conference on Information and Communication Technology Convergence (ICTC), Jeju, Republic of Korea, 19–21 October 2016; pp. 287–291.
15. Taurshia, A.; Kathrine, J.W.; Shibin, D. Prognostic Views on Software Defined Networks Based Security for Internet of Things. Commun. Comput. Inf. Sci. 2019, 1116, 100–116.
16. Joshi, K.D.; Kataoka, K. pSMART: A lightweight, privacy-aware service function chain orchestration in multi-domain NFV/SDN. Comput. Netw. 2020, 178, 107295.
17. Paolucci, F.; Cugini, F.; Castoldi, P.; Osinski, T. Enhancing 5G SDN/NFV Edge with P4 Data Plane Programmability. IEEE Netw. 2021, 35, 154–160.
18. Vijayakumar, P.; Bose, S.; Kannan, A. Chinese remainder Theorem based centralised group key management for secure multicast communication. IET Inf. Secur. 2014, 8, 179–187.
19. Ezekiel, S.; Divakaran, D.M.; Gurusamy, M. Dynamic attack mitigation using SDN. In Proceedings of the 2017 27th International Telecommunication Networks and Applications Conference (ITNAC), Melbourne, VIC, Australia, 22–24 November 2017; pp. 1–6.
20. Babiceanu, R.F.; Seker, R. Cyber resilience protection for industrial internet of things: A software-defined networking approach. Comput. Ind. 2019, 104, 47–58.
21. Babiceanu, R.F.; Seker, R. Cybersecurity and resilience modelling for software-defined networks-based manufacturing applications. In Service Orientation in Holonic and Multi-Agent Manufacturing; Springer: Berlin/Heidelberg, Germany, 2017; Volume 694, pp. 167–176.
22. Piedrahita, A.F.M.; Gaur, V.; Giraldo, J.; Cardenas, A.A.; Rueda, S.J. Leveraging Software-Defined Networking for Incident Response in Industrial Control Systems. IEEE Softw. 2017, 35, 44–50.
23. Madhawa, S.; Balakrishnan, P.; Arumugam, U. Employing invariants for anomaly detection in software defined networking based industrial internet of things. J. Intell. Fuzzy Syst. 2018, 35, 1267–1279.
24. Mansour, A.; Azab, M.; Rizk, M.R.M.; Abdelazim, M. Biologically-inspired SDN-based Intrusion Detection and Prevention Mechanism for Heterogeneous IoT Networks. In Proceedings of the 2018 IEEE 9th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON), Vancouver, BC, Canada, 1–3 November 2018; pp. 1120–1125.
25. Chung, J.; Jung, E.-S.; Kettimuthu, R.; Rao, N.S.; Foster, I.T.; Clark, R.; Owen, H. Advance reservation access control using software-defined networking and tokens. Future Gener. Comput. Syst. 2018, 79, 225–234.
26. Sharma, P.K.; Park, J.H.; Jeong, Y.-S.; Park, J.H. SHSec: SDN based Secure Smart Home Network Architecture for Internet of Things. Mob. Networks Appl. 2019, 24, 913–924.
27. Demetriou, S.; Zhang, N.; Lee, Y.; Wang, X.; Gunter, C.A.; Zhou, X.; Grace, M.C. HanGuard: SDN-Driven Protection of Smart Home WiFi Devices from Malicious Mobile Apps. In Proceedings of the 10th ACM Conference on Security and Privacy in Wireless and Mobile Networks, Boston, MA, USA, 18–20 July 2017; Volume 2017, pp. 122–133.
28. Caprolu, M.; Raponi, S.; Di Pietro, R. FORTRESS: An efficient and distributed firewall for stateful data plane SDN. Secur. Commun. Netw. 2019, 2019, 6874592.
29. Ge, M.; Hong, J.B.; Yusuf, S.E.; Kim, D.S. Proactive defense mechanisms for the software-defined Internet of Things with non-patchable vulnerabilities. Future Gener. Comput. Syst. 2018, 78, 568–582.
30. Zarca, A.M.; Bernabe, J.B.; Skarmeta, A.; Calero, J.M.A. Virtual IoT HoneyNets to mitigate cyberattacks in SDN/NFV-Enabled IoT networks. IEEE J. Sel. Areas Commun. 2020, 38, 1262–1277.
31. Wang, S.; Gomez, K.; Sithamparanathan, K.; Asghar, M.R.; Russello, G.; Zanna, P. Mitigating ddos attacks in sdn-based iot networks leveraging secure control and data plane algorithm. Appl. Sci. 2021, 11, 929.
32. Wani, A.; Revathi, S.; Khaliq, R. SDN-based intrusion detection system for IoT using deep learning classifier (IDSIoT-SDL). CAAI Trans. Intell. Technol. 2021, 6, 281–290.
33. Aslam, M.; Ye, D.; Tariq, A.; Asad, M.; Hanif, M.; Ndzi, D.; Chelloug, S.A.; Elaziz, M.A.; Al-Qaness, M.A.A.; Jilani, S.F. Adaptive Machine Learning Based Distributed Denial-of-Services Attacks Detection and Mitigation System for SDN-Enabled IoT. Sensors 2022, 22, 2697.

34. Burmester, M.; Desmedt, Y. A secure and efficient conference key distribution system. Lect. Notes Comput. Sci. 1995, 950, 275–286.
35. Waller, D.; Harder, E.; Agee, R. Key Management for Multicast: Issues and Architectures. 1999. Available online: https://www.rfc-editor.org/rfc/rfc2627 (accessed on 9 March 2023).
36. Ku, W.C.; Chen, S.M. An improved key management scheme for large dynamic groups using one-way function trees. In Proceedings of the 2003 International Conference on Parallel Processing Workshops, Kaohsiung, Taiwan, 6–9 October 2003; Volume 2003, pp. 391–396.
37. Xu, X.; Wang, L.; Youssef, A.; Zhu, B. Preventing collusion attacks on the one-way function tree (OFT) scheme. In Applied Cryptography and Network Security; Springer: Berlin/Heidelberg, Germany, 2007; Volume 4521, pp. 177–193.
38. Sun, Y.; Chen, M.; Bacchus, A.; Lin, X. Towards collusion-attack-resilient group key management using one-way function tree. Comput. Netw. 2016, 104, 16–26.
39. Festijo, E.; Jung, Y.; Peradilla, M. Software-defined security controller-based group management and end-to-end security management. J. Ambient. Intell. Humaniz. Comput. 2019, 10, 3365–3382.
40. Mansour, A.; Malik, K.M.; Alkaff, A.; Kanaan, H. ALMS: Asymmetric Lightweight Centralized Group Key Management Protocol for VANETs. IEEE Trans. Intell. Transp. Syst. 2021, 22, 1663–1678.
41. Tiloca, M.; Dini, G.; Rizki, K.; Raza, S. Group Rekeying Based on Member Join History; Springer: Berlin/Heidelberg, Germany, 2019; Volume 19, pp. 343–381.
42. Zhang, S.; Han, S.; Zheng, B.; Han, K.; Pang, E. Group Key Management Protocol for File Sharing on Cloud Storage. IEEE Access 2020, 8, 123614–123622.
43. Tamizhselvan, C. A novel communication-aware adaptive key management approach for ensuring security in IoT networks. Trans. Emerg. Telecommun. Technol. 2022, 2022, e4605.
