A STEP TOWARDS BUILDING TRUSTWORTHY WIRELESS SENSOR NETWORK

Synopsis of thesis submitted

in partial fulfillment of the requirements for the award of the

Master of Technology

in

Computer Science & Engineering

(under the Dual-Degree Programme)

by

Himanshu Goyal

17CS02011

Under the supervision of

Dr. Sudipta Saha

School of Electrical Sciences

Indian Institute of Technology Bhubaneswar

Orissa, India - 752050

Abstract

Smart living would become an inevitable part of the near future because of the ever-growing demand due to the exponential rise in the population and the need to balance such demand with the limited natural resources. True smart living is fundamentally determined by the available services from the smart systems such as smart-city, smart-building, smart-home, intelligent transportation systems, precision agriculture, intelligent environmental monitoring, smart-grid, and many others. Internet-of-Things (IoT)[1]can be considered the primary enabler of such smart living for humanity. Every such intelligent system fundamentally thrives upon massive decentralized coordination and cooperation among many independent devices. The performance of an IoT system, thus, significantly depends on how well the devices can talk to each other and how smoothly they can coordinate together and execute the necessary tasks.

However, the growing concerns of several attacks[2, 3, 4, 5, 6]ranging from data integrity to data privacy have raised severe concerns about adopting IoT-based smart systems. These attacks could potentially cause a serious threat to the end-users thus affect the quality of service. Therefore, it has become more important for these systems to be secure, as well as reliable. Moreover, in certain cases, such systems also need to be able to preserve privacy too. However, because of the participation of many devices having low processing capability as well as high energy constraints, unlike traditional systems, it becomes much more difficult

to achieve these goals. Therefore, we are interested in building a *"trustworthy network"* that is robust against intentional/non-intentional device failures and can provide the service of carrying out computation over the data held by a set of devices privately and securely.

In this work, particularly we view an IoT system as a massive collection of low-power devices spread over a wide area where each device can do some work, communicate with each other, and have limited energy. Moreover, we also consider that some devices are controlled by adversaries interested in gaining control over the network or want the network to deviate from the desired goal. The main weakness of an IoT system is the resource constraints in the devices. However, we perceive the massive number of devices in IoT as their strength. We view it as a massively distributed system and plan to compensate for the resource limitation in the devices with collaborative computing where device-to-device communication plays a vital role. To appropriately exploit the power of such a massive size, we deviate from the traditional asynchronous transmission-based communication strategies to in-parallel time slotted based communication strategies. In this work, we mainly focused on achieving Byzantine fault tolerance in IoT networks and privacy-preserving data-aggregation among the participating nodes.

Finally, we evaluate our proposed in both simulation and emulation settings. We simulate the protocols over MSPSim and ns-2 simulator. We also experiment with the implementations in emulation environments with sensor nodes having 802.15.4 compliant radios with ARM architecture.

Keywords: Privacy-Preserving Data aggregation, Threshold Cryptography, Practical Byzantine Fault tolerance, Broadcast Communication, Data Sharing: One-to-all, Many-to-Many, All-to-All,etc.

Dissemination of Research Results

1. *Himanshu Goyal*, Sudipta Saha. Multi-party computation in IoT for Privacy Preservation - Accepted in 42nd **IEEE International Conference on Distributed Computing Systems (ICDCS)**, 2022, Bologna, Italy.

2. *Himanshu Goyal*, Sudipta Saha. LiPI: Lightweight Privacy-Preserving Data Aggregation in IoT - Under Review, IoT Journal.

3. *Himanshu Goyal*, Sudipta Saha. Practical Byzantine Fault-tolerance for Internet-of-Things - Under Review.

4. *Himanshu Goyal*, Sudipta Saha. DivConMPC: Divide and Conquer based Privacy Preserving Multi-Party Computation in IoT - To be submitted in the conference publication.

Synopsis

1. Objective

The contemporary period has seen the rise of Internet-of-Things (IoT) devices to serve people with various applications such as smart metering, urban traffic monitoring, weather monitoring, and so on. Low Power Wide Area Networks (LPWAN) technical advancements provide promising solutions for effectively realizing these existing applications while also opening the door to sophisticated applications such as Edge Computing, Machine Learning, and Artificial Intelligence. We anticipate that most services in the future will significantly rely on LPWAN because it incorporates features from LoRa, NB-IoT, and SigFox. Consequently, the usage of smart systems has increased in the recent past quite drastically because of such intriguing technologies. As a result of it, we are getting more dependent on these smart systems. However, as people's quality of life improves, so do the risks associated with dependent applications, such as data leakage and the integrity of the underlying network in the event of a failure. So far, it is generally established that it is simple to construct protocols that are secure from the outside world through the usage of traditional cryptographic techniques. However, when we have to create a secure solution that is robust against failures and internal and external adversaries simultaneously, the scenario changes entirely and becomes non-trivial despite the usage of cryptography. The typical network structure possible in the

real-world can be visualized as shown in Fig. 1. We need protocols that can provide sufficient guarantees while working in such practical settings. Keeping this as the focal point of this work, we broadly focus on the following two domains.

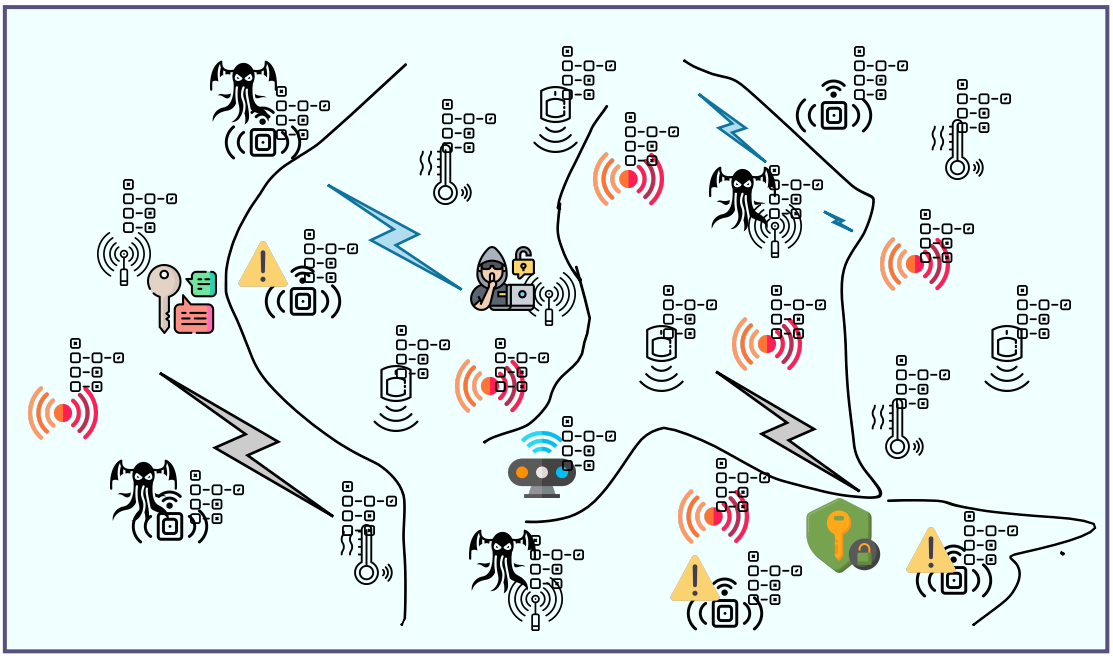

Figure 1: *Overview of an IoT/WSN network while operating in practical settings*

Security and Privacy: A system being secure, as well as trustworthy, may not be able to preserve the privacy of the data from individual nodes. The problem of privacy in IoT becomes very important when the sensed data have a relation with specific users. However, preserving privacy under massive IoT systems is very challenging, especially under multi-hop settings. Sensitive user data may not be safe to reveal as its propagation doesn't limit to only one node. The data shared by each node is the same for all the nodes. If it's in plain text format, then all intermediate nodes between the source and sync node can gather relevant information about this sensitive data. If it's not in plain text, then the sync node can play the role of the potential information seeker. The available standard solutions

assume sync node(s) as trusted third parties, and each node sends its sensed value to it with an aim to carry out some distributed learning task. Even if messages are encrypted, and intermediate nodes don't have access to them, Sync nodes can decrypt them and see the raw data shared by each node and interpret them locally to gain more information that clearly breaches node privacy. However, some of these applications will substantially use sensitive data to achieve the desired goal. It is understandable from past experience that the exposition of such data (amount of power consumption, Data used in Health monitoring) can have undesired consequences. Therefore, it becomes necessary to provide such services to users at the same comfort without compromising their privacy. Moreover, It has been observed that some of these services need to compute aggregation statistics over the data sensed by the participating nodes. Such aggregation becomes critical when it is being carried out on particular sensitive data. The traditional cryptographic techniques have provided us with optimal encryption and decryption techniques. However, such data obfuscation techniques ensure data security only when it is in the transmission or storage. Therefore, In order to perform any analytics over such data, the data eventually needs to be decrypted at the central server to perform the final aggregation calculation. Moreover, the central server can certainly become a single point of failure, as shown in [7]. Thus, it necessitates a system in place that protects the security of data both while it is in transmission and computation.

However, modern cryptography provides the service of Secure computation that allows a set of parties to compute some joint function of their private inputs while guaranteeing privacy (i.e., the parties learn the output and nothing more) and correctness (meaning the output is correctly distributed). Recently several solutions based on Privacy Enhancing Technologies(PETs) like Homomorphic Encryption(HE), Differential Privacy(DP), and Secure Multi-party Computation (SMPC)

have been proposed in the literature. However, we believe that techniques like HE are inappropriate for IoT devices due to their low computation power. Moreover, we believe such techniques involve high computation with an increase in the number of nodes in an underlying network. Therefore, we seek MPC-based techniques to be the best fit for such low-power devices. Despite their low computation overhead, they frequently require interaction with other participants. Consequently, we believe that to realize the complete essence of MPC-based solutions for IoT/WSN networks, we require efficient communication protocols that could quickly achieve the requisite data sharing needs.

Consequently, we believe this gap can be bridged in the context of IoT networks with the usage of efficient data sharing protocols like [8, 9, 10, 11] in asynchronous domain and flooding based communication mechanisms like [12, 13, 14, 15, 16]. Works like [15] perform in-network aggregation but do so on plain-text data, which directly breaches the node privacy. Moreover, their aggregation can work only for idempotent functions. Consequently, we seek an aggregation protocol that can guarantee: *Security, Privacy, Robustness, and Scalability.*

Trust: Secure communication protocols alone cannot provide trust in a system. For example, nodes in the systems can behave maliciously even after complying with security requirements in the case of applications like distributed database replication. The applications running on top of a flooding protocol assume every node is honest and thus would purely depend on information what their neighbors are saying and assume them to be true blindly. In the case of sensitive, e.g., data replication) applications, an adversary or a group of adversaries can inject false data to divert the network from having a single decision. Byzantine fault tolerance protocols can potentially help in alleviating the problem of failed or maliciously behaving nodes. It may therefore be realized that agreement is important for reliable decentralized applications. The way these applications leverages the dis-

tributed computing power of IoT nodes is quite motivating and intriguing. These technological elevations make it more likely that malicious attacks and software errors will occur regularly. Thus, it has now become a fundamental requirement to build resilient network services that can withstand a wide range of failure types in distributed systems. However, the incorporation of Byzantine Fault tolerance seems to be a more promising direction toward the adoption of IoT-based decentralized applications. Currently, many applications need extensive coordination among their counterparts to do the defined job more precisely in low-power wireless networks. These applications can range from coordination among industrial controllers(Smart Grid) to mission-critical systems like a swarm of Unmanned Aerial Vehicles(UAVs). For example, The UAVs could be on some mission and would like to compute the exact target location with a common agreement to harm the enemy effectively, a deviation of which can lead to a significant loss. The prior proposed solution [15] in the domain IoT for achieving consensus only manages crash failures. They restricted themselves to handling Byzantine failures as their underlying protocol is designed for in-network data aggregation, whereas we need all-to-all data sharing for byzantine failures. Thus, we plan to derive trustable consensus and aggregation protocols that can potentially help for any network-wide operations.

2. Contribution

The work completed throughout the course of this thesis may be classified as follows:

- Broad classification of security attacks and node failures possible in decentralized IoT networks and implementation of IoT-based services that need a specific level of security and privacy along with a
- Determination of the appropriate number of transmissions/re-transmissions required from each node to achieve the desired degree of overall network coverage.
- Developed an efficient Byzantine Fault-tolerant consensus mechanism to achieve trust in IoT networks amidst classified failures. Optimized the proposed BFT consensus protocol as compared to naive execution utilizing the underlying network characteristics.
- Achieved pair-wise secret keys for all pairs of participating nodes using a single run of all-to-all data sharing.
- A privacy-preserving single-round non-interactive protocol for performing aggregate statistics over the data of massive IoT/WSN networks is proposed. The protocol is made safe and robust against node dropouts.
- Avoided the usage of encryption techniques to make the protocols suitable for the use of resource-constrained devices. Proposed the scalable versions of the developed techniques using temporal and spatial group divisions, supporting a large number of IoT devices.
- A thorough assessment of the developed protocols in simulation and emulation environments.

3. Conclusion

While in operation, IoT-based smart systems must give adequate assurances such as security, privacy, resilience, etc. The absence of either of these undoubtedly poses several risks to both users and the network itself. However, meeting such standards is not easy because an practical IoT network consists of several devices, as shown in,1 and behaves differently from typical wired networks. The key challenges are how devices can efficiently interact with one another to achieve any stated set of goals in the face of internal or external prospective adversaries. As a result, ensuring the security guarantees for a network comprised of heterogeneous IoT devices is difficult. However, we believe such characteristics are necessary and need to be fulfilled for critical applications. Therefore, we consider all requirements and develop our protocols with these objectives in mind. We specifically created protocols for computing aggregate statistics on the data of participating IoT nodes while maintaining privacy. In addition, we provide a service to make IoT networks reliable/trustworthy by enabling computation to occur in the face of Byzantine failures. To make it time and energy-efficient, we introduced a couple of optimizations over the naive strategy based on the observation that we do not need the highest degree of privacy protection or fault tolerance for many practical cases.

4. Proposed Organisation of the Thesis

The organization of the thesis is as follows:

- The first chapter emphasizes the need of developing trustworthy IoT networks and difficulties involved in desigining such a network that can simultaneously defend itself from internal and external threats. It includes thorough information about the objectives and the contributions made during

this work. It also includes the experimental platforms used for testing and validation.

- The second chapter discusses the underlying communication protocols, which we employ to throughout the work. Moreover, it provides the literature survey about the existing works related to objectives defined in Chapter 1.

- Later on, the thesis is broadly divided into two parts and address questions like: *how can we achieve fault tolerance in IoT based smart systems, and how can we perform computation on participating node data without disclosing any information about the data itself?*

- The third chapter provides the necessary background regarding Byzantine fault tolerance, and challenges in porting PBFT to WSN/IoT systems, and our proposed Byzantine fault tolerance consensus mechanism, show how it is scalable for IoT/WSN systems. It also provides an in-depth evaluation of the proposed strategy, and a comparison with a naive implementation of the strategy.

- The fourth chapter demonstrates that using cryptography for encryption and decryption does not ensure data privacy when the underlying data is necessary for computation. It emphasizes the risks of IoT data leakage and the importance of privacy-preserving data processing services. Furthermore, we demonstrate how to compute aggregate statistics on sensor nodes' data without revealing any information about sensed data. In addition, we assess and compare our proposed scheme to state-of-the-art solutions.

- Chapter 5 summarizes the novelty of the work, also indicating how it is in alignment with the current standards.

- The chapter 6 includes a direction toward handling active adversaries. Finally, it also briefs the limitations of the work and the scope for future work.

Bibliography

[1] L. Atzori, A. Iera, and G. Morabito, "The internet of things: A survey," *Computer Networks*, vol. 54, no. 15, pp. 2787–2805, 2010.

[2] M. Conti, A. Dehghantanha, K. Franke, and S. Watson, "Internet of things security and forensics: Challenges and opportunities," 2018.

[3] F. B. de Oliveira, *On Privacy-Preserving Protocols for Smart Metering Systems: Security and Privacy in Smart Grids*. Springer, 2016.

[4] E. L. Quinn, "Privacy and the new energy infrastructure," *Available at SSRN 1370731*, 2009.

[5] S. Tan, D. De, W.-Z. Song, J. Yang, and S. K. Das, "Survey of security advances in smart grid: A data driven approach," *IEEE Communications Surveys & Tutorials*, vol. 19, no. 1, pp. 397–422, 2016.

[6] M. T. Moghaddam and H. Muccini, "Fault-tolerant iot," in *International Workshop on Software Engineering for Resilient Systems*, pp. 67–84, Springer, 2019.

[7] M. A. Uddin, A. Stranieri, I. Gondal, and V. Balasubramanian, "A survey on the adoption of blockchain in iot: Challenges and solutions," *Blockchain: Research and Applications*, vol. 2, no. 2, p. 100006, 2021.

[8] O. Gnawali, R. Fonseca, K. Jamieson, M. Kazandjieva, D. Moss, and P. Levis, "Ctp: An efficient, robust, and reliable collection tree protocol for wireless sensor networks," *ACM Trans. Sen. Netw.*, vol. 10, dec 2013.

[9] T. Winter, P. Thubert, A. Brandt, J. Hui, R. Kelsey, P. Levis, K. Pister, R. Struik, J.-P. Vasseur, and R. Alexander, "Rpl: Ipv6 routing protocol for low-power and lossy networks," tech. rep., 2012.

[10] J. Lu and K. Whitehouse, *Flash flooding: Exploiting the capture effect for rapid flooding in wireless sensor networks*. IEEE, 2009.

[11] M. Maróti, B. Kusy, G. Simon, and A. Lédeczi, "The flooding time synchronization protocol," in *Proceedings of the 2nd International Conference on Embedded Networked Sensor Systems*, SenSys '04, (New York, NY, USA), p. 39–49, Association for Computing Machinery, 2004.

[12] F. Ferrari, M. Zimmerling, L. Mottola, and L. Thiele, "Low-power wireless bus," in *SenSys, 2012*.

[13] C. Herrmann, F. Mager, and M. Zimmerling, "Mixer: Efficient many-to-all broadcast in dynamic wireless mesh networks," in *SenSys, 2018*.

[14] M. Mohammad and M. C. Chan, "Codecast: Supporting data driven in-network processing for low-power wireless sensor networks," in *IPSN, 2018*.

[15] O. Landsiedel, F. Ferrari, and M. Zimmerling, "Chaos: Versatile and efficient all-to-all data sharing and in-network processing at scale," in *SenSys, 2013*.

[16] S. Saha, O. Landsiedel, and M. C. Chan, "Efficient many-to-many data sharing using synchronous transmission and tdma," in *DCOSS, 2017*.