Secure Energy Constrained LoRa Mesh Network

Derek Heeger[1,2][0000−0002−4666−8538], Maeve Garigan[3][0000−0003−4242−3901], Eirini Eleni Tsiropoulou[2][0000−0003−1322−1876], and Jim Plusquellic[2][0000−0002−1876−117X]

[1] Sandia National Labs, Albuquerque NM, USA
[2] University of New Mexico, Albuquerque NM, USA
{heegerds,eirini,jplusq}@unm.edu
[3] Roper Solutions Inc, Las Cruces NM, USA
maeve@ropertag.com

Abstract. LoRa (Long Range) is a low-power wide-area network technology well-suited for Internet of Things (IoT) applications. In this paper, LoRa is used in a cattle monitoring application where an ad-hoc mesh network is configured to collect GPS and accelerometer data from cattle-worn sensors and relay the collected data to a base station. Free-range cattle monitoring is a challenging application since the battery-powered sensors must be small and energy efficient, and enable data communications over long distances from unpredictable locations. We propose novel changes to the existing LoRa mesh network protocols that minimize energy consumption by using global time synchronization enabled by GPS sensors and a concurrent transmission property unique to LoRa. The mesh routing phase efficiently occurs during every data collection period, making this approach ideal for networking highly mobile sensors. We integrate efficient authentication and encryption techniques in the data exchange operations to prevent spoofing and to provide confidentiality in the message exchanges between the sensors and the base station. The performance of the proposed secure implementation is compared to an equivalent insecure implementation. Multiple cattle distribution scenarios are constructed and compared to evaluate the energy consumption of the proposed scheme.

Keywords: LoRa · Mesh Networks · Cattle Monitoring.

1 Introduction

In recent years, the Internet of Things (IoT) paradigm has expanded rapidly into commercial, industrial and consumer applications. This expansion has driven a corresponding need for energy efficient battery-powered networked devices. The energy consumed during data communications is a significant fraction of the total energy consumption, and is a particular concern for IoT applications in rural areas, where transmission over long distances is necessary due to a lack of networking infrastructure. Low-power wide-area network (LPWAN) technologies such as LoRa (Long Range), Sigfox, and Narrowband IoT (NB-IoT) [1] offer a distinct advantage for rural IoT by providing enhanced energy efficiency and long range data communications.

LoRa uses a proprietary spread spectrum modulation similar to chirp spread spectrum (CSS) modulation to achieve high noise immunity at the expense of low data rates. LoRa has configurable parameters such as spreading factor (SF), bandwidth, and error coding rates, which enable trade-offs between range and noise immunity [2]. LoRa is used as the transport layer for the LoRa Wide Area Network (LoRaWAN) networking protocol in which LoRa-enabled devices communicate directly with LoRa gateways. Given its low cost to build and operate, LoRa has received a great deal of interest from the academic and amateur radio communities, and has been used in various IoT applications, such as smart cities, industrial IoT, agriculture, smart metering, and environmental monitoring [3].

In this paper, we investigate a novel LoRa ad-hoc mesh network architecture for tracking and monitoring the location and activity of free-range cattle. Within the proposed system, battery-powered sensors are attached to the cattle and periodically collect and transmit GPS and accelerometer data to a base station. The long transmission distances and physical obstacles (such as rolling hills, trees and other cattle) require that the sensor network be configured as a mesh, allowing collected data to be relayed from sensor to sensor before reaching the base station. Data transfer between the base station and the sensors is bi-directional and must be accomplished with ultra-low energy consumption. The proposed system introduces a protocol that enables secure and energy-optimized data communication over distances that exceed those specified for LoRaWAN. The proposed framework uses GPS to time synchronize all sensors in the network to precise wake-up times, enabling the configuration of an infrequent, secure, and coherent data exchange network that minimizes energy consumption. Applications that use the proposed system will benefit from the increased data transmission range and improved reliability in packet delivery while experiencing a minimal increase in energy consumption.

1.1 State of the Art & Motivation

A wireless mesh network (WMN) is a network communication paradigm wherein client devices can act as message relays and increase the probability of a successful packet delivery [4]. Mesh network architectures exist for multiple IoT standards, including WiFi, Bluetooth, and Zigbee [5]. Reactive and proactive routing protocols have been proposed within WMNs to define how the system discovers message routing. In proactive routing protocols, the IoT devices maintain routing tables to represent the entire network topology, while in the reactive protocols, a multi-hop route is created on-demand, thus reducing the routing overhead [5]. WMNs have a route discovery phase to generate an internal forwarding table based on the message destination. The routes remain valid until the IoT device status changes (e.g., changes position or goes offline) which initiates a maintenance phase. WMNs can consume significant amounts of energy due to the complexities of maintaining and updating the routing tables.

Various mesh architectures have been proposed for LoRa. A LoRa mesh network is introduced in [6] to monitor underground infrastructure, and consists of stationary sensors that are configured as dedicated relay nodes to LoRaWAN gateways and use GPS time synchronization to minimize energy consumption. The authors develop a LPWAN based on the LoRa physical layer (LoRa PHY) and demonstrate that it overcomes the transmission limitations (i.e., medium-range underground connectivity and time stamping of data packets) of the LoRaWAN standard in underground applications. The LoRaWAN standard supports only single-hop communication, which is addressed in [7] where multi-hop networking between LoRa gateways is proposed as a means of extending coverage. The proposed multi-hop routing protocol integrates Hybrid Wireless Mesh Protocol (HWMP) and the Ad-hoc On-Demand Distance Vector Routing (AODV) technologies into the LoRaWAN specification. Issues related to signal attenuation, particularly those related to obstacles and non-line-of-sight transmission, are addressed in [8], where a mesh network using the LoRa PHY is developed and its packet delivery performance is evaluated. The authors demonstrate that their scheme provides a better packet delivery ratio than an alternative star-network topology, although the proposed scheme lacks security and low power operation.

Concurrent transmissions of IoT devices in multi-hop LoRa mesh networks are investigated in [9] and [10]. In [10], a scheme is proposed for improving packet delivery by introducing timing offsets between the packets. In [9], scalability issues are investigated in large-scale LoRa networks where the authors show that LoRa networks configured with static settings and a single sink are not scalable. They propose a scheme which uses multiple sinks and dynamic communication parameter settings as an alternative. In [11], a network configuration is proposed wherein a forwarder-node is introduced between the IoT device and the gateway to improve the range and quality of LoraWAN communications. That work is extended in [12] using a Destination-Sequenced Distance Vector (DSDV) routing protocol where IoT devices are configured to transmit packets to intermediate relay nodes that forward the packets to LoRa gateways.

1.2 Contributions & Outline

The aforementioned work on LoRa mesh networks focuses on performance and does not address network security within LoRa mesh networks. Moreover, only limited work exists on extending the effective communication range of LoRa devices while minimizing energy consumption. Our work addresses these gaps by introducing a custom ad-hoc network architecture based on the LoRa PHY that provides ultra-low power operation while maintaining advanced capabilities within the network infrastructure, including mesh networking and a framework for authentication and encryption of sensor data using an efficient packet structure.

This work is motivated by a realistic free-range cattle monitoring application that uses battery-powered sensors to collect GPS and accelerometer data and is transmitted via LoRa to a base station [13]. The challenges associated with monitoring free-range cattle using IoT devices are summarized as follows:

1. Cattle are highly mobile and travel long distances to unpredictable locations in rural, off-grid areas, making the communication link unreliable.

2. Cattle act as large dielectrics and can absorb a considerable amount of radio-frequency transmission energy, making the IoT device communications range dependent on cattle orientation.

3. The sensor package must be small and lightweight, requiring a small battery, which creates a highly energy constrained scenario.

We propose a LoRa mesh network that uses adjacent cattle as relays to transmit sensor data to the LoRa base station. Typical mesh network protocols are unsuitable for our cattle monitoring application because they consume significant energy, perform poorly with mobility, and are insecure. Our mesh network architecture overcomes these shortfalls and makes the following novel contributions:

1. Our system leverages GPS time synchronization and LoRa concurrent transmission capabilities to efficiently collect data from ultra-low power sensors distributed over a large geographic area.

2. Our system integrates light-weight encryption and authentication security functions into a LoRa mesh network to prevent packet sniffing, data spoofing, and intelligent denial of service (DoS) attacks.

3. Our system is applied to a novel free-range cattle monitoring application, which introduces significant challenges to ensuring reliable packet delivery and ultra-low energy consumption. The system will be experimentally validated in a cattle ranch environment in the near future using a sensor prototype developed by Roper Solutions, Inc. (Fig. 1).

The remainder of this paper is organized as follows: Section 2 describes the mesh network, Section 3 provides a detailed performance analysis, Section 4 describes the proposed security features, and Section 5 concludes the paper.

2 System Overview

The proposed system will be integrated into a cattle monitoring sensor shown in Fig. 1. The custom sensor platform includes a GPS receiver, an accelerometer, and a LoRa module for data communication. The sensor package includes a low capacity battery that is recharged from a solar panel. The current consumption of the battery-powered sensor with the LoRa receiver enabled can exceed 5 mA, creating a significant power drain over time. The sensors can be configured to remain in an ultra-low power mode, however this makes them unable to receive messages. To maintain receptivity and ultra-low power consumption, the sensors are periodically and simultaneously awakened, which requires global time synchronization among all sensors in the mesh network. We use GPS time synchronization with guard bands to achieve this goal and avoid techniques that exclusively maintain time with oscillators as they are prone to error due to drift. We define an *event* as a global awakening of all sensors and a complete data exchange between the LoRa base station and the sensors. Events occur at fixed time intervals, e.g., once every 1-4 hours, and the sensors awaken every 0.25 hours to collect position and health information and re-synchronize with the global clock.

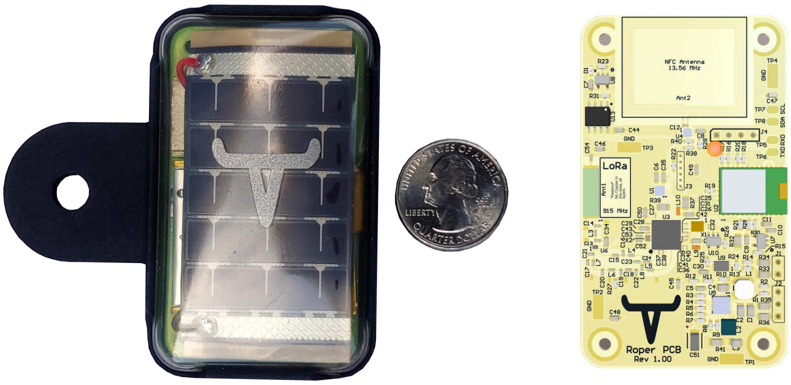


Fig. 1: (a) Roper cattle sensor in housing. (b) Graphic of the sensor board PCB.

2.1 System Behavior

The physical location of the cattle determines the number of hops required for the sensor data transmitted during an event to reach the LoRa base station. A series of R rounds is defined within the time frame of an event, with each round subdivided into synchronization (synch) frames and data frames. Each round defines the time interval in which data is collected from a subset of the sensors. For example, during Round 1, the base station collects data from sensors that have a direct communication path (Fig. 2). In Rounds 2 and 3, the base station collects data from sensors that are one and two mesh hops away, respectively. Each round progresses one hop further from the previous round, until all sensors have responded.

The base station is responsible for transmitting synch packets to the sensors in each round, and they respond with data packets that travel back to the base station. An illustration of a packet sequence consisting of synch packets S_x and sensor data packets $Data_x$ is shown in Fig. 3. The synch packet initiates the data transmission operation from the sensors and enables the route-finding algorithm to determine a set of feasible routes. The data frames contain a time slot for each sensor, enabling each of them to communicate their unique GPS and accelerometer data to the base station.

The number of rounds required depends on the distribution of the sensors. For example, if every sensor was within range of the base station, only one round would be required. If there are C cattle spaced equally at the communication range boundaries, C rounds would be required to collect all the data. An exception occurs when one or more sensors are unable to respond. This scenario can result in empty rounds unless a stop condition is incorporated. Two possible stop criteria are limiting the number of rounds to a fixed upper bound or terminating after a round occurs in which no data is collected.

2.2 Packet Structure

The synch packet formats used in the insecure (top) and secure (bottom) versions of the proposed LoRa mesh network are shown in Fig. 4. The packet includes

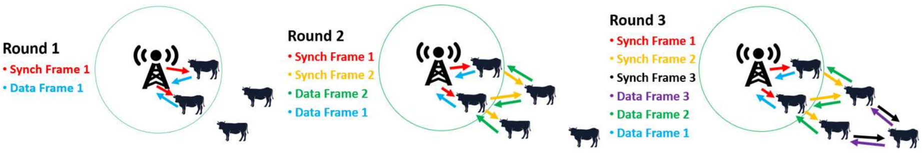


Fig. 2: Illustration of communication pathways within the LoRa mesh network in the context of Events and Rounds.

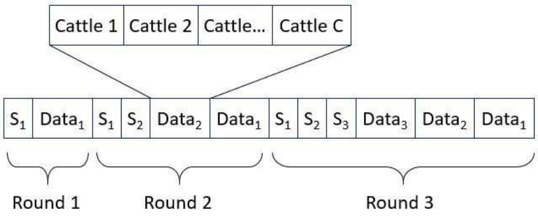


Fig. 3: Example sequence of synchronization and sensor data packets from multiple rounds during an event.

a Base ID to identify the base station that the packet originated from. The *Round* field is incremented at the end of each round and the Hop field is incremented at each mesh hop. The $Bit - mapped\ Response$ field records which cattle have responded, where one bit is allocated for each cow, making the packet size dependent on C. A cyclic redundancy check (CRC) code is appended to the insecure packet to enable detection of packet transmission errors. The secure version includes a digital signature or message authentication code MAC and a time stamp field $Time$, which increase the packet size by 20-bytes over the insecure version. The digital signature is encrypted using a 128-bit version of the Advanced Encryption Standard (AES) algorithm, commonly referred to as AES Cipher-based Message Authentication Code (AES-CMAC). The purpose of the security related components of the packet are discussed further in Section 4.

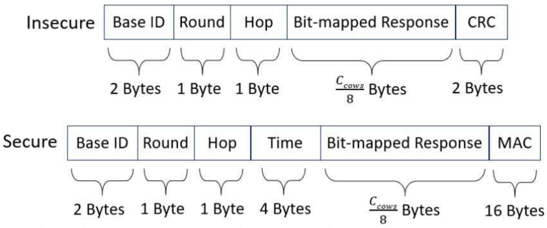


Fig. 4: Insecure (top) and secure (bottom) synchronization packet formats.

The insecure and secure data packet formats for individual cattle are shown in Fig. 5. The Base ID, Hop Count, and CRC serve the same purpose as described above for the synchronization packet. The Herd ID indicates which cow the data came from. The payload portion of the data packet consists of 25-bytes of information related to the cow's current location and recent activity. The payload portion of the secure packet is extended to 32-bytes, and includes a 4-byte time stamp and 0-padding as needed, to match the input width of the encryption algorithm, AES-128.

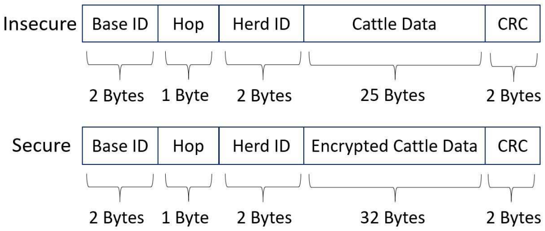
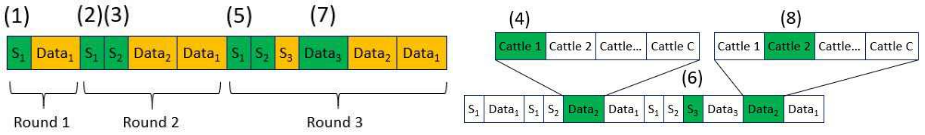


Fig. 5: Insecure (top) and insecure (bottom) data packet formats.

2.3 Transmit and Receive Logic

The LoRa base station enables ad-hoc mesh networking using the following message exchange protocol:

1. Transmit a synch packet containing the bit-mapped response set to 0.
2. Wait for data packets to arrive from the responding cattle sensors.
3. Confirm message authenticity from each data packet (secure version only).
4. Update the bit-mapped response by setting fields to 1 for the cattle sensors that it has received data from and transmit a new synch packet.
5. Repeat Steps 2 through 4 until the stop condition is met.



(a) Receive logic

(b) Transmit logic

Fig. 6: Illustrations showing example transmit and receive actions carried out by the proposed protocol.

The behavior of the sensor protocol is described using the example sequence of events in Fig. 6a and 6b, where (a) shows behavior by the receiving portion (Receive logic) and (b) shows the behavior of the transmitting portion (Transmit logic). The figures are annotated with numbers to indicate the time order in which the events occur. The following describes the actions taken by a typical sensor in the network and assumes that the sensor is attached to Cattle 1 which is located 2 hops away from the base station.

1. The sensor listens for synch packets until one is received. It listens in Round 1, designated as S_1, but no packet is received so it returns to sleep.
2. The sensor awakens at the beginning of Round 2 and listens for a synch packet (S_1), but again no packet is received. It continues to listen for all synch packets in a given round before returning to sleep.
3. The sensor receives a synch packet in the second time slot of Round 2, designated as S_2, which it received from another sensor one hop away.
4. In response, the sensor transmits a data packet containing its GPS and accelerometer data during the Cattle 1 time slot of $Data_2$ and then returns to sleep mode.

5. The sensor awakens at the beginning of Round 3, and receives another synch packet S_2. The bit-mapped response within the packet contains a 1 in the Cattle 1 field, which indicates that the base station received the data packet. If the bit was not set, indicating a packet loss, it would re-transmit the Cattle 1 sensor data in the $Data_2$ slot. It also acts as a relay node because the round number is greater than the hop count. The sensor deduces the process has not terminated because the bit-mapped fields are not all set to 1.
6. When acting as a relay, the sensor must broadcast the synch packet during S_{h+1}. Fig. 6b shows the sensor re-broadcasting the synch packet during S_3.
7. The sensor then listens for broadcasts from other sensors during $Data_{h+1}$ ($Data_3$ in this case) and will act as a relay if it receives any data.
8. If another sensor transmits during $Data_3$, e.g., Cattle 2, it will broadcast this in $Data_2$, during Cattle 2's time slot, which will move the data from Cattle 2's sensor one hop closer to the base station. Note that it is possible for multiple cattle to engage in a (re)transmission operation simultaneously during any given time interval. This condition is referred to as a concurrent transmission which is acceptable because LoRa receivers lock onto the strongest signal.
9. The sensor repeats this process until the synch packet indicates that the data collection process has completed, either because all bit-mapped fields are set to 1 or a stop condition has been met.

3 Analysis

LoRa settings can be changed to increase or decrease communication range with a corresponding penalty or benefit to transmission time. Fig. 7a plots the transmission time (T_{Synch}) as a function of the SF and bandwidth to send an insecure and secure synch packet, illustrating the modest overhead associated with the proposed security extension. As discussed earlier, the security extension adds to the length of the network packets and corresponding transmission time, as shown here. Similarly, Fig. 7b shows the time for all C cattle to transmit one data packet (T_{Data}), as a function of herd size, C, under different LoRa settings, with and without the security extension.

The energy consumption for a sensor to carry out the protocol operations over the time interval defined by a single event is given by Eq. 1, where h is the hop count, R is the total number of rounds, C is the total number of cattle in a herd, and n is the number of sensors with the same or fewer hop counts. P_t and P_r are the transmit and receive power respectively.

$$\begin{aligned} E_{device}(h,R,n) = {} & (T_{synch}(R-h) + T_{data}(C-n)/C)P_t \\ & + (T_{synch}h(\frac{h+1}{2} + R - h) + T_{data}(R-h))P_r \end{aligned} \tag{1}$$

The best case energy consumption scenario is defined by Eq. 2 and occurs when all cattle sensors are within range of the base station.

$$E_{best} = T_{data}P_t + 2T_{synch}P_r \tag{2}$$

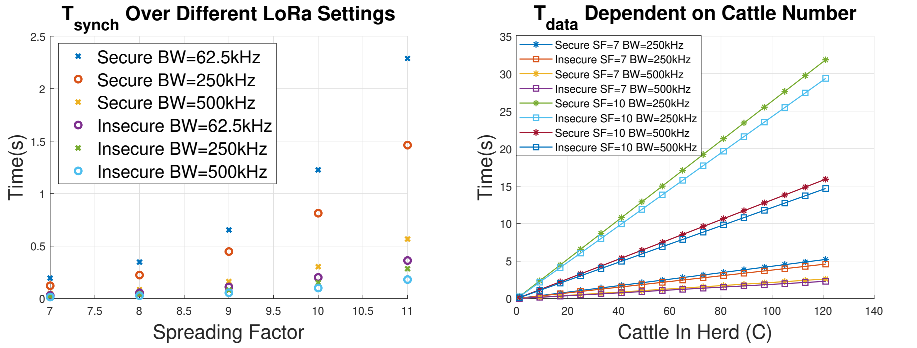


Fig. 7: (a) Transmission time for a synch packet over various LoRa settings, (b) Transmission time for a data window dependent on the number of cattle.

The worst case energy consumption (Eq. 3) occurs for the sensor closest to the base station, in an arrangement where all sensors are spaced equally in a straight line from the base station. Here, the base station must execute C rounds to collect the complete data set.

$$E_{worst} = C((T_{data} + T_{synch})P_t + (T_{synch} + (C-1)T_{data})P_r) \tag{3}$$

The total energy consumption for all sensor nodes is defined as the sum of the individual consumption from all the cattle sensors.

To evaluate the performance of our proposed mesh topology, we created a custom simulation model with the cattle sensors distributed in a 1-dimensional space (1-D). Existing simulation tools, such as NS3, could not accurately model the energy consumption performance due to the different states that the sensors operate in. The performance in the 1-D distribution scenario represents the worst case even in an actual 2-dimensional (2-D) scenario. The following parameters are used in our analysis: average $P_t = 330mW$ and $P_r = 15.9mW, C = 128, SF = 9, BW = 250kHz$, and error coding rate 1.25.

We present the energy consumption for the linear distribution of cattle sensors in Fig. 8a, where the number of cows per hop is indicated by the right axis. The transmit and receive energy is plotted as individual curves along with the total energy consumed per device at each hop in the mesh (x-axis). The devices located closer to the base station are tasked with relaying more data and therefore consume more energy. From the graph, the peak energy consumption for sensors located at the first hop is 6 J. This allows for approximately 450 mesh events before recharging is required, assuming a small 2.7 kJ (200 mAh) rechargeable lithium-ion battery is used. An alternative uniform distribution is shown in Fig. 8b where the sensors are distributed equally such that (C/R) cattle are located at every hop. The linear distribution more closely models a real-world cattle distribution. This is true because the base station will typically be placed at the cattle's water source, a location to which the cattle will cluster.

We now assess how energy consumption scales as a function of herd size and spreading. Fig. 9a shows how the energy consumption scales as the maximum

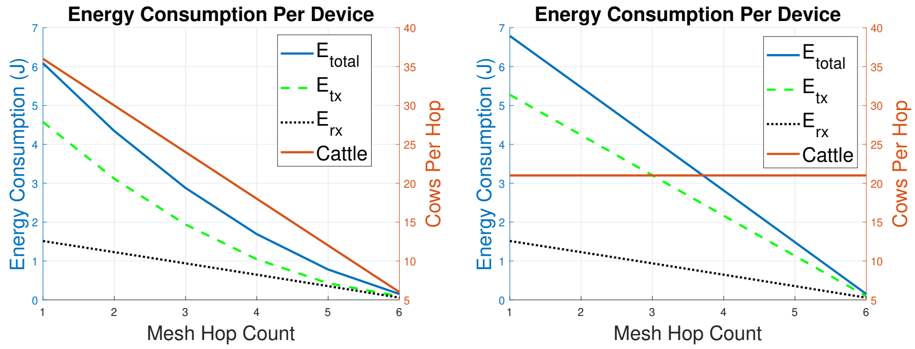


Fig. 8: (a) Energy consumption if cattle have linear distribution, (b) Energy consumption if cattle have a uniform distribution.

hop count increases. Here, we assume the size of the herd is fixed at 128 and examine increasingly wider distributions among the herd. The average and maximum power consumption of the sensor is plotted under the linear and uniform distribution models. These results indicate that the relationship between energy consumption and hop count is linear, suggesting that a strategy which restricts maximum hop count could conserve energy, but introduces the risk that some sensors may be unable to communicate with the base station. Fig. 9b shows that the average and maximum energy consumption scales linearly with the size of the herd. The energy load on the sensors at the first hop, indicated by $\mathrm{E}_{\mathrm{max}}$, scales at a higher rate than the average consumption of the herd ($\mathrm{E}_{\mathrm{avg}}$).

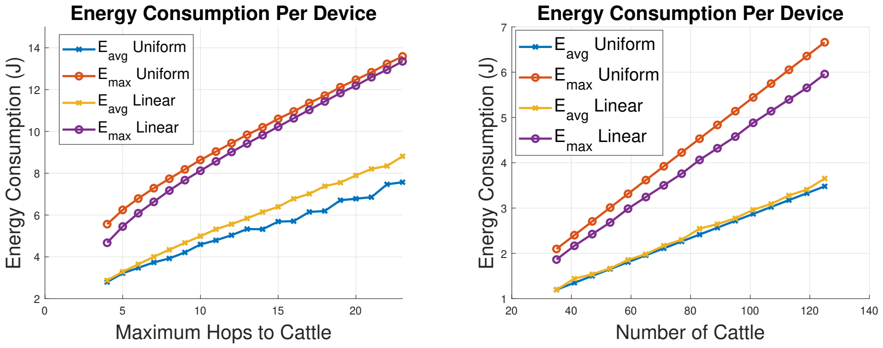


Fig. 9: (a) Energy consumption per device as a function of the number of hops, (b) Energy consumption for six hops as a function of herd size.

4 Security

The primary goals of a secure system are to ensure data privacy and to prevent false impersonation of sensors. The proposed security extension to the cattle monitoring application utilizes two 128-bit keys including a herd key K_h and cattle-specific key K_c for use in AES-based encryption and authentication operations. K_c is unique to every sensor while K_h is common to the entire herd. We assume the base station is able to securely communicate with a server to gain access to the keys.

AES is used to encrypt data using K_c before transmission through the LoRa network. K_c is stored privately in non-volatile memory on each sensor preventing intermediate sensor nodes from decrypting data that they relay to the base station. Each encrypted data packet includes a 4-byte time stamp which serves as a message authentication code (MAC) to enable the base station to detect malicious modifications to the transmitted data. The MAC prevents malicious actors from carrying out spoofing attacks by making it nearly impossible for them to create valid encrypted data packets.

The synch packet is authenticated with a MAC using K_h. Thus, every sensor in the network can validate the authenticity of the fields in the packet. This prevents a simple DoS attack where a malicious actor broadcasts a fake synch packet indicating the base station has received data from all sensors, which in turn triggers all sensors to enter sleep mode until the next event. The 4-byte time stamp makes the MAC unique over successive authentication operations, thus preventing replay attacks where adversaries capture and attempt to reuse previously transmitted MACs.

Encryption prevents malicious actors from eavesdropping on cattle-specific sensor data transmissions if they do not possess the sensor's encryption key. However, an adversary can apply invasive techniques or side-channel analysis methods to extract sensor-specific keys [14,15]. If an adversary is able to extract K_h and K_c using such methods, they would be able to create valid data packets and impersonate the base station. However, because K_c is unique to each sensor, they would be unable to impersonate sensors from other cattle.

In the event that a sensor goes entirely offline because the cow or its sensor moves out of range (for example, in the case of theft), a key update operation would be required to maintain security within the network. The ability to periodically update sensor keys will prevent adversaries who engage in key extraction attacks from compromising network security. Secure re-keying involves selectively updating K_h on every sensor. Distributing $\mathrm{K}_{\mathrm{h,new}}$ can be accomplished by sending a packet encrypted by the base station with K_c to each device. The key update process requires a distinct packet format and message exchange protocol beyond those defined earlier in this paper.

5 Conclusion

In this work, we propose a novel LoRa secure mesh network architecture designed for battery-powered, GPS-enabled IoT devices and other ultra-low power applications. Our architecture is applied to a cattle monitoring sensor network and addresses unique challenges related to cattle mobility and unpredictability. The design uses device-level GPS to enable time synchronized ad-hoc mesh routing operations performed by all networked devices. We define the packet structure and transmit/receive logic of the proposed protocol, and assess its performance and energy consumption over a variety of cattle distribution models to illustrate its suitability for energy constrained IoT applications. Security extensions are described to provide privacy in data transmissions and authentication between devices in the network. A prototype cattle sensor has been developed and future work will evaluate our secure mesh network architecture using data collected from cattle in a ranch environment.

Acknowledgments

We would like to thank Kevin Nichols for the support and Mike Partridge for the motivation. Sandia National Laboratories is a multi-mission laboratory managed and operated by National Technology and Engineering Solutions of Sandia, LLC, a wholly-owned subsidiary of Honeywell International, Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA-0003525. The research of Dr. Eirini Eleni Tsiropoulou was conducted as part of NSF CRII-1849739.

References

1. Mekki, K., Bajic, E., Chaxel, F., Meyer, F.: A comparative study of lpwan technologies for large-scale iot deployment. ICT express **5**(1) (2019) 1–7
2. SX1276, L.: 77/78/79 datasheet, rev. 4 (2015)
3. Sarker, V., Queralta, J.P., Gia, T., Tenhunen, H., Westerlund, T.: A survey on lora for iot: Integrating edge computing. In: 2019 Fourth International Conference on Fog and Mobile Edge Computing (FMEC), IEEE (2019) 295–300
4. Hossain, E., Leung, K.K.: Wireless mesh networks: architectures and protocols. Springer (2007)
5. Cilfone, A., Davoli, L., Belli, L., Ferrari, G.: Wireless mesh networking: An iot-oriented perspective survey on relevant technologies. Future Internet **11**(4) (2019) 99
6. Ebi, C., Schaltegger, F., Rüst, A., Blumensaat, F.: Synchronous lora mesh network to monitor processes in underground infrastructure. IEEE Access **7** (2019) 57663–57677
7. Lundell, D., Hedberg, A., Nyberg, C., Fitzgerald, E.: A routing protocol for lora mesh networks. In: 2018 IEEE 19th International Symposium on" A World of Wireless, Mobile and Multimedia Networks"(WoWMoM), IEEE (2018) 14–19
8. Lee, H.C., Ke, K.H.: Monitoring of large-area iot sensors using a lora wireless mesh network system: Design and evaluation. IEEE Transactions on Instrumentation and Measurement **PP** (03 2018) 1–11
9. Bor, M.C., Roedig, U., Voigt, T., Alonso, J.M.: Do lora low-power wide-area networks scale? In: Proceedings of the 19th ACM International Conference on Modeling, Analysis and Simulation of Wireless and Mobile Systems, ACM (2016) 59–67
10. Liao, C.H., Zhu, G., Kuwabara, D., Suzuki, M., Morikawa, H.: Multi-hop lora networks enabled by concurrent transmission. IEEE Access **5** (2017) 21430–21446
11. Velde, B.: Multi-hop lorawan: including a forwarding node (2017)
12. Dias, J., Grilo, A.: Lorawan multi-hop uplink extension. Procedia computer science **130** (2018) 424–431
13. Roper: Revolutionizing beef production. https://www.ropertag.com/.
14. Skorobogatov, S.: Flash memory 'bumping'attacks. In: International Workshop on Cryptographic Hardware and Embedded Systems, Springer (2010) 158–172
15. Zhou, Y., Feng, D.: Side-channel attacks: Ten years after its publication and the impacts on cryptographic module security testing. IACR Cryptology ePrint Archive **2005**(388) (2005)