Performance Trade-offs in IoT Uplink Networks under Secrecy Constraints

Avik Sengupta, *Student Member, IEEE*, Ahmed Abdelhadi, *Senior Member, IEEE*,
T. Charles Clancy, *Senior Member, IEEE*

***Abstract*—We investigate the performance of Internet-of-Things (IoT) networks under passive attacks from eavesdroppers capable of monitoring individual links. An IoT network with multiple sensor classes is studied where every sensor class has a local access point (LAP) which are connected to one or more small cell base-station access points (SAP) which in turn are connected to a central cloud access point (CAP). The CAP interfaces the IoT network to the Cloud Radio Access Network which serves the users who request sensor readings. We propose a unique attack resilient IoT sensor reporting model based on IoT traffic characteristics and study the performance of this system under strict latency and secrecy constraints.**

***Index Terms*—IoT, Latency, Uplink, Eavesdropper, Secrecy.**

I. Introduction

The proliferation of heterogeneous wireless network architectures as well as a multitude of radio access techniques have paved the way for a fully connected Internet-of-Things (IoT) paradigm. IoT is envisioned to create a bridge between machine-type communications and wireless data networks [1], [2]. IoT networks consist of a very large number of low power devices which report sensor readings over the network. For example, users are able to connect to their home devices over wireless networks to monitor their current states. While modern wireless networks are mostly limited by the ability to handle large volumes of multimedia data, such data generally does not have very strict latency constraints. IoT networks on the other hand, generally handle a large number of single digit sensor readings which have very strict latency constraints especially over multiple hops. Thus a latency centric analysis of IoT networks is in order. Furthermore, IoT networks generally have asymmetric traffic being mostly uplink heavy with mostly control signaling in the downlink.

Since the nature of data communication over the IoT networks is potentially of a confidential nature, the security of such data is an important design aspect in IoT networks. Recent works in [3], [4] have studied secrecy in downlink cache-enabled networks. Conversely in this work, we present a latency-centric study of secrecy in uplink IoT networks. We develop an attack resilient system framework for sensor data reporting on the IoT uplink. Under passive attacks from an eavesdropper capable of intercepting transmissions on the uplink, we provide countermeasures to such attacks and study the cost of security in terms of latency and backhaul rate.

II. IoT Network Model

We consider an IoT network where users, requesting data from different sensor classes, from one edge of the network and the sensor classes form the opposite edge. The network model is illustrated in Figure 1. Under this setting, we consider uplink data communication from the sensors to the users under secrecy constraints. We outline a system model resilient to passive attacks from an eavesdropper in the sequel.

A. Network Connectivity

We consider a set of N *local access points* (LAP) $\mathcal{L}_1, \mathcal{L}_2, \ldots, \mathcal{L}_N$. An IoT sensor class is a cluster of IoT sensors served by one LAP. Each LAP is connected to one or more *small cell access points* (SAP). We assume that the IoT network has a total of S SAPs denoted by $\mathcal{S}_1, \mathcal{S}_2, \ldots, \mathcal{S}_S$. In the following discussion, the terms IoT class and LAP are used interchangeably.

The connectivity between the LAPs and the SAPs is defined by a bipartite graph $\mathcal{G} = (\mathcal{S}_{1:S}, \mathcal{L}_{1:N}, E)$, where the edge $(\mathcal{S}_s, \mathcal{L}_n) \in E$ for $s \in 1, \ldots, S$ and $n \in 1, \ldots, N$. We further define a probabilistic coverage model, where probabilities $\gamma_{s,n}$ denote the probability of the SAP $\mathcal{S}_s$ being connected to the $n-$th IoT class LAP $\mathcal{L}_n$. We observe that

$$\sum_{n=1}^{N} \gamma_{s,n} = 1, \quad \forall s \in \{1, 2, \ldots, S\}, \tag{1}$$

i.e., the probability distribution is over the set of N sensor classes. Furthermore, note that the connection probabilities also account for physical layer characteristics of the network including fading, shadowing and relative location (separation) of SAPs and LAPs[1]. The set of SAPs are connected to a central cloud access point (CAP) through finite capacity backhaul links. The CAP is considered to be a cellular base station (e.g., eNodeB in LTE) which forms the gateway for the IoT sensor network to connect to a cloud radio access network (C-RAN). The users wanting access to the IoT sensor readings requisition their demands through the C-RAN to the CAP. Thus, it is imperative that the CAP is able to serve the users with their requested information with minimal latency. To this end, we next define the end-to-end communication policy on the uplink between the IoT LAPs and the CAP.

B. Uplink Data Transmission Policy

In this work we concentrate on the IoT uplink model from the LAP to the CAP. IoT networks generally consist of machine-type nodes which report sensor readings to users. Thus, the traffic is usually uplink-heavy with mostly control signaling on the downlink. It is further envisioned that the latency of transmission is the limiting factor in these networks rather than the volume of data traffic since most sensor readings have finite expiry times.

The authors are with the Hume Center for National Security and Technology & Department of ECE, Virginia Tech, Blacksburg, VA 24060, USA. Email: {aviksg, aabdelhadi, tcc}@vt.edu. This research is based upon work supported by the National Science Foundation under Grant No. 1134843.

[1]The values $\gamma_{s,n}$ can be considered as the probability of a SAP $\mathcal{S}_s$ being connected to a LAP $\mathcal{L}_n$ averaged over multiple random realizations of the connectivity graph $\mathcal{G}$ thereby accounting for topology/link changes over time.

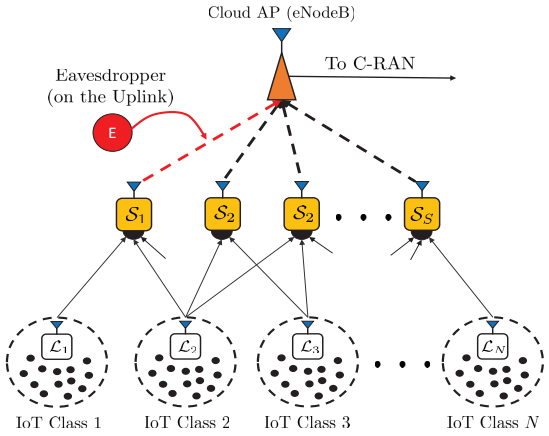


Fig. 1. System Model for Uplink Data Communication in IoT.

In order to incorporate the traffic characteristics of IoT networks, we assume that user requests from the C-RAN are served directly from the CAP with data already available in its buffer. Further, since the CAP is a central node, we assume it has a large enough buffer size to store reports from all N IoT classes under its service. Based on this assumption, it is pertinent to study the uplink data communication between the LAPs and the CAP under varying latency constraints such that a *fresh set of sensor readings* is always available at the CAP buffer to serve user requests. We next define the sensor reporting policy for the IoT network. The LAP-CAP uplink communication policy is defined as $\pi = (\pi_{\mathsf{E}}, \pi_{\mathsf{F}})$, where π_{E} is an encoding policy at the LAPs and π_{F} is a forwarding policy at the SAPs. The policies are designed to be resilient to eavesdroppers and the associated protocols are defined next.

1) Encoding Policy π_{E}: The encoding of the sensor data is performed at each IoT class LAP for transmission to the SAPs serving them. To this end, we first define a composite sensor reading namely the *sensor report*, SR_n at the LAP $\mathcal{L}_n$, which consists of readings from multiple sensors within the $n-$th IoT sensor class. The users request these composite reports from CAP through the C-RAN. Each LAP collects data packets from its connected sensor nodes and encodes these packets using a rateless MDS channel code e.g., raptor codes [5]. Assume that each report SR_n is encoded into rateless coded packets such that any r packets suffice to decode the report at any end user or CAP. Similar to prior work in [2], we also assume that each report SR_n has an expiry time Δ_n. Δ_n is defined as the time, from generation of the report, to the time at which it expires and is not valid for futher use.

2) Forwarding Policy π_{F}: We next consider the action of the SAPs in the uplink policy. Each SAP, $\mathcal{S}_s$, $\forall s \in \{1, \ldots, S\}$, connects to the LAP $\mathcal{L}_n$, $\forall n$, with probability $\gamma_{s,n}$, to retrieve at most r encoded packets from the LAP. Each SAP then processes and forwards the encoded packets to the CAP with a transmit power budget of P. We define the number of retrieved packets normalized by r as the fraction $m_{s,n} \in [0, 1]$. We define as t_n, the time taken by each SAP to process (retrieve and transmit) a single packet from sensor class $n \in \{1, \ldots, N\}$ and forward to the CAP. In our model, we allow for different processing times for different classes since, without loss of generality, each IoT class may use different radio access protocols, thereby requiring different times for processing and forwarding. In the case of a homogeneous network, the times could be same for all classes. As an example, if an SAP retrieves 5 packets from LAP $\mathcal{L}_1$, the delay in processing is $5t_1$. The processing time t_n is similar to a buffering time where the SAP collects all the packets and then transmits them together to the CAP. There is a *decodability constraint* at the CAP such that it needs to receive at least r packets from each sensor report SR_n such that it can decode the messages for servicing user requests. The total processing time at each SAP is defined as follows:

$$T_p(s) = \sum_{n=1}^{N} m_{s,n}\ r\ t_n, \qquad \forall s \in \{1, \ldots, S\}. \tag{2}$$

$T_p(s)$ should be such that across all SAPs, the processing time is cumulatively large enough to process at least rN packets within the latency constraints. This is required due to the decodability constraint at the CAP. Furthermore, an upper limit of $T_p(s)$ can be the time taken to completely process all required rN packets at each SAP. Thus, we have

$$\frac{r}{S}\sum_{n=1}^{N} t_n \leq T_p(s) \leq r\sum_{n=1}^{N} t_n, \qquad \forall s \in \{1, \ldots, S\}. \tag{3}$$

Subject to restrictions on $T_p(s)$ related to the end-to-end latency, we seek an answer to the following question: *what is the optimal fraction of packets that each SAP needs to retrieve from the LAPs?* Since multiple SAPs can forward packets from the same IoT class (LAP) to the CAP, transmission cooperation at the SAPs is the main design goal. We aim to study such cooperation under passive attacks from an eavesdropper. To this end, we first define two different system frameworks and consequently address them under a threat model with counteractive secrecy constraints.

III. A Latency Centric IoT Uplink Framework

In this section, we present two main IoT frameworks which aid a latency centric study of the IoT uplink model discussed in Section II. First, we consider a network model where the backhaul link is rate-limited (i.e., fixed low-rate backhaul link). Under this setting, we aim to study the trade-off between the end-to-end latency of the system vs. the total processing time, $T_p(s)$, at each SAP. Next, we consider a latency-limited backhaul link, where we need to meet a fixed latency budget to maintain data freshness under varying backhaul rate. Under this setting, we aim to study the trade-off between the backhaul rate and the processing time $T_p(s)$ under strict latency constraints. We next develop each framework separately.

A. Rate-Limited Backhaul Network

Consider a rate-limited backhaul link between each SAP and the CAP with a fixed rate $\log(P)$ bits/sec for ease of exposition. The latency over these links for transferring data from the SAPs to the CAP is then proportional to the amount of data, $m_{s,n}$, fetched by each SAP from their connected sensor LAPs. Thus, the end-to-end latency[2] for each SAP can be written as:

$$\mathsf{L(s)} = \sum_{n=1}^{N} r\ m_{s,n}\left(t_n + \frac{1}{\log(P)}\right). \tag{4}$$

[2]Here we have assumed that the SAPs from the N IoT sensor classes at a fixed latency and the LAP-SAP links are not rate limited. Thus we do not account for this latency in the formulation choosing instead to adjust the $T_p(s)$ accordingly to account for it.

Further, based on the coverage probability, $\gamma_{s,n}$, of the SAPs, we can write an expected end-to-end latency for each SAP as:

$$\mathsf{L_{exp}(s)} = \sum_{n=1}^{N} \gamma_{s,n}\ r\ m_{s,n} \left(t_n + \frac{1}{\log(P)} \right). \tag{5}$$

The expected latency is thereby dependent on the fraction of retrieved packets and their related processing times at the SAPs subject to a total processing time constraint at each SAP. Further, the end-to-end decodability constraint dictates that the CAP receive at least r packets from each sensor class. Finally, we define a parallel access protocol highlighting the method in which the CAP accesses data from the SAPs. In this access protocol, the SAPs can send their data in parallel to the CAP. As a result the end-to-end latency of this system is limited by the maximum latency faced by any of the constituent SAPs.

We next formulate a joint optimization problem to minimize the end-to-end latency of the parallel access system. This problem entails the SAPs to jointly fetch content by accounting for the network topology. Let

$$\mathbf{M} = \left[m_{s,n},\ {}^{s\in 1,\ldots,S}_{n\in 1,\ldots,N} \right]$$

be an $S \times N$ data retrieval matrix. Then the minimum system latency can be expressed as the solution of the following minimization problem:

$$\underset{m_{s,n}\in\mathbf{M}}{\text{minimize}} \quad \left[\max_{s\in 1,2,\ldots,S} \sum_{n=1}^{N} \gamma_{s,n}\ r\ m_{s,n} \left(t_n + \frac{1}{\log(P)} \right) \right] \tag{6}$$

$$\text{subject to:} \quad \sum_{s=1}^{S} m_{s,n} \geq 1, \qquad \forall n \in 1,2,\ldots,N, \tag{7}$$

$$\sum_{n=1}^{N} r t_n m_{s,n} \leq T_p(s), \quad \forall s \in 1,2,\ldots,S, \tag{8}$$

Let the solution to the system be $\mathsf{L_{exp}(opt)}$. The minimization in (6) aims to minimize the worst case end-to-end latency in the system. The constraints (7)-(8) are explained as follows: The first constraint (7) follows directly from the decodability constraint of SR_n at the CAP. The second constraint (8) is based on the per SAP processing time constraint $T_p(s)$. This is an equivalence of the buffer processing time and enables the APs to fetch more content based on the allowable processing time. Finally, the formulation in (6)-(8) assumes that none of the sensor reports expire within the time taken for transmission under the constraint (8) i.e., $\Delta_n \leq \min_{s\in 1,\ldots,S} \mathsf{L_{exp}(s)}$. Note that $T_p(s)$ and transmission power P are system parameters which can be varied to study the latency performance. In this formulation we are interested in the $\mathsf{L_{exp}(opt)}$ vs. $T_p(s)$ trade-off. The optimization problem in (6) is based on minimizing the maximum of linear S linear terms. Thus, we can equivalently reformulate (6) as an LP by introducing an auxiliary variable $\mathsf{L_{Aux}}$, as follows:

$$\underset{m_{s,n}\in\mathbf{M}}{\text{minimize}} \quad \mathsf{L_{Aux}} \qquad \text{subject to:} \tag{9}$$

$$\sum_{n=1}^{N} \gamma_{s,n}\ r\ m_{s,n} \left(t_n + \frac{1}{\log(P)} \right) \leq \mathsf{L_{Aux}}, \quad \forall s \tag{10}$$

in addition to constraints (7)-(8). The problem in (9) is a linear program subject to linear constraints and hence can be solved optimally by use of numeric solvers.

B. Latency-limited Backhaul Network

Consider a latency-limited backhaul network, where the link between each SAP and the CAP is not rate limited but is limited by a total latency constraint. In this setting, we consider a total latency constraint T_{total} such that

$$T_{\mathsf{total}} \geq T_p(s) + T_b(s), \qquad \forall s \in 1,\ldots,S, \tag{11}$$

where $T_b(s)$ is the latency on the backhaul link from $\mathcal{S}_n$ to the CAP. Further, we have $\Delta_n \leq T_{\mathsf{total}}$ i.e., the latency constraint ensures data freshness at the CAP. Thus, under this setting, we have a strict latency constraint on the end-to-end transmission from the LAPs to the CAP. As a result, based on amount of data downloaded by each SAP, the rate of the backhaul transmission varies since the link has fixed latency. The backhaul rate due to each SAP can be expressed as

$$\mathsf{R(s)} = \frac{\sum_{n=1}^{N} r\ m_{s,n}}{T_{\mathsf{total}} - T_p(s)} \ \text{ packets/unit time.} \tag{12}$$

Thus under probabilistic connectivity model, the expected backhaul rate can be expressed as

$$\mathsf{R_{exp}} = \sum_{s=1}^{S} \frac{\sum_{n=1}^{N} r\ \gamma_{s,n}\ m_{s,n}}{T_{\mathsf{total}} - T_p(s)}. \tag{13}$$

Again, an optimization problem similar to (6) can be formulated to minimize the expected backhaul rate:

$$\underset{m_{s,n}\in\mathbf{M}}{\text{minimize}} \quad \mathsf{R_{exp}} \tag{14}$$

$$\text{subject to:} \quad \sum_{s=1}^{S} m_{s,n} \geq 1, \qquad \forall n \in 1,\ldots,N, \tag{15}$$

$$\sum_{n=1}^{N} r t_n m_{s,n} \leq T_p(s), \quad \forall s \in 1,\ldots,S, \tag{16}$$

$$T_{\mathsf{total}} \geq T_p(s) + T_b(s), \quad \forall s \in 1,\ldots,S. \tag{17}$$

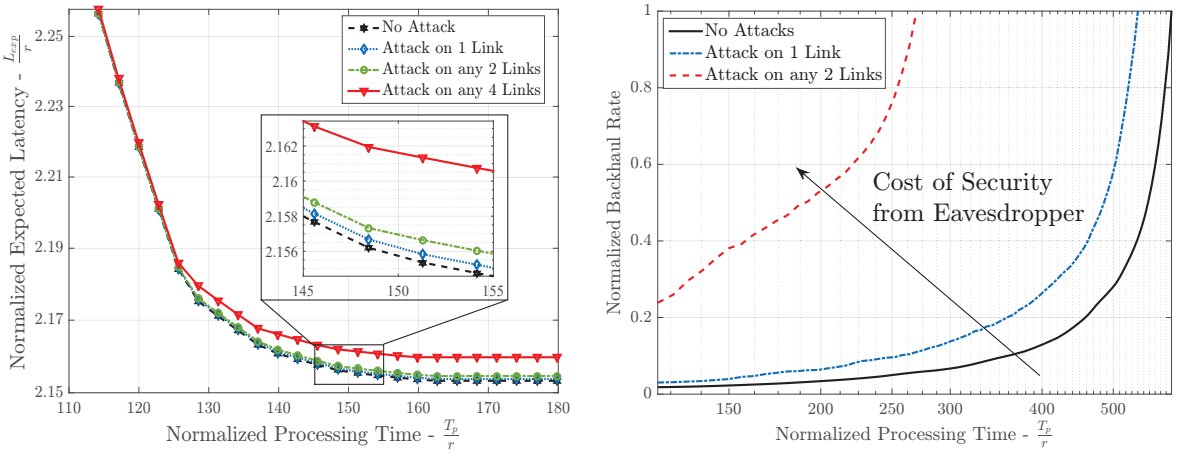
Similar to the previous framework, (14) is a linear program which can be solved numerically. In this setting, we are interested in the optimal expected backhaul rate vs. processing time i.e., $\mathsf{R_{exp}(opt)}$ vs. $T_p(s)$ trade-off. We next look at the attack models in the IoT network in the presence of an eavesdropper.

IV. Secrecy in IoT: Attack Models

Since the uplink data communication in the IoT networks consists of sensor reports $\mathsf{SR}_n,\ \forall n$, which potentially contain classified information, network security is an important paradigm. A main design goal of the proposed system model is resilience against external attacks. The proposed MDS coding of sensor reports SR_n is a means of adding robustness and redundancy in the links against passive eavesdroppers and leads to simpler countermeasures for secrecy. To this end, we study possible attacks on the IoT uplink and derive the related secrecy constraints under which the attacker is unable to decode any sensor report.

A. Passive Eavesdropping on the Backhaul Link

This is an eavesdropper based passive attack scenario and is illustrated in Figure 1. In this attack model, an eavesdropper, E, is capable of observing and intercepting transmissions one or more corrupt SAP to CAP link. The SAP or the CAP are unaware of which link is intercepted. However, the system



(a) (b)

Fig. 2. Passive attack by an eavesdropper on (a) rate-limited backhaul link and (b) latency-limited backhaul link.

is aware of the number of links which can be attacked in the worst case. Thus, to achieve secrecy over this potentially compromised link, the SAP needs to ensure that r packets from any one sensor are never transmitted over the compromised links. Let $\mathcal{B}_c$ be the set of attacked links. If the eavesdropper is capable of intercepting transmissions on any $k \leq S$ links, then we have the cardinality of the set

$$|\mathcal{B}_c| = \binom{S}{k} \quad \text{backhaul links.}$$

Thus, in order to ensure that the eavesdropper does not decode any sensor report with a passive attack on links in the set $\mathcal{B}_c$, we have the following simple secrecy constraint:

$$\sum_{\ell \in \mathcal{B}_c} m_{\ell,n} < 1, \quad \forall n \in 1, \ldots, N. \tag{18}$$

Note that the constraint (18) takes a simple form due to the attack-resilient design of the system model. Solving the linear programs (9) and (14) subject to the additional constraint (18) entails a latency centric study of the cost of security in the IoT uplink network.

V. Simulation Results

In this section, we provide more insight into the uplink IoT network transmission under secrecy constraints for a network with $N = 52$ IoT classes and $S = 5$ SAPs. The network connectivity probabilities $\gamma_{s,n}$ are generated according to a zipf power law distribution with random exponents between $0.25 - 0.5$. This was chosen to model distance-based connectivity and a more intricate modeling is left for future work. We assume that the constraint $T_p(s)$ is equal for each SAP and is varied between the limits in (3) to study the trade-offs. The number of packets r is a system parameter and as a result, we select the $r\ t_n$ to belong to the set $\{1, 3, 7, 9\}$ time units. Figure 2(a) shows the latency vs. processing time trade-off for the rate-limited backhaul framework under different attacks from an eavesdropper. We plot the expected latency normalized by the number of packets r. It can be seen that for the rate-limited links, the effect of attacks in terms of end-to-end latency is minimal i.e., even when 2 out of 5 links is attacked, the cost in terms of latency is very low. This is owing to the relatively loose latency constraints in the rate-limited framework.

On the other hand, for the network with total latency constraint, T_{total}, Figure 2(b) shows the normalized expected backhaul-rate vs. processing time trade-off. In this case, we set the minimum allowed backhaul latency $T_b^{\min} = \left(\sum_{n=1}^{N} r\ t_n\right)/S$ while the total latency constraint is set as $T_{\text{total}} = 2\left(\sum_{n=1}^{N} r\ t_n + T_b^{\min}\right)$. Note that the chosen parameters are selected to make a meaningful initial study of the network and are by no means exhaustive. Under this strict constraint, we see that attacks on the backhaul links have a much more pronounced effect. The simple mitigation techniques make the problem infeasible for higher values of T_p. This is intuitive since a high T_p implies a very low T_b thereby increasing the rate. As attacks increase, reliable transmission cannot be achieved under the T_b budget for the backhaul links.

VI. Conclusions and Future Work

In this letter, we presented a latency centric study of an IoT uplink network under passive attack from an eavesdropper. We showed that under rate-limited backhaul links, the resilience to attacks on multiple links is good. For latency-limited backhaul links, the cost of security in terms of rate is relatively high. Future work in this paradigm will account for more complex counter measures for passive attacks such that secrecy can be achieved at a potentially lower cost. Furthermore, active attacks from IoT classes will be considered where rogue LAPs can flood the SAP with spurious packets thereby crippling the network. The study of backhaul rate and latency and the corresponding cost of secrecy is an open problem.

References

[1] N. Nikaein, M. Laner, K. Zhou, P. Svoboda, D. Drajic, M. Popovic, and S. Krco, "Simple traffic modeling framework for machine type communication," in *IEEE ISWCS*, Aug 2013, pp. 1–5.

[2] S. Vural, P. Navaratnam, N. Wang, C. Wang, L. Dong, and R. Tafazolli, "In-network caching of internet-of-things data," in *IEEE International Conference on Communications (ICC)*, June 2014, pp. 3185–3190.

[3] A. Sengupta, R. Tandon, and T. C. Clancy, "Fundamental limits of caching with secure delivery," *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 2, pp. 355–370, Feb 2015.

[4] F. Gabry, V. Bioglio, and I. Land, "On edge caching with secrecy constraints," *arXiv: 1602.06156*, 2016. [Online]. Available: http://arxiv.org/abs/1602.06156

[5] A. Shokrollahi, "Raptor codes," *Information Theory, IEEE Transactions on*, vol. 52, no. 6, pp. 2551–2567, June 2006.