2015 IEEE 12th International Conference on Mobile Ad Hoc and Sensor Systems

Black SDN For The Internet of Things

Shaibal Chakrabarty, Daniel W. Engels, *Senior Member, IEEE*, Selina Thathapudi

***Abstract*—In this paper, we present Black SDN, a Software Defined Networking (SDN) architecture for secure Internet of Things (IoT) networking and communications. SDN architectures were developed to provide improved routing and networking performance for broadband networks by separating the control plain from the data plain. This basic SDN concept is amenable to IoT networks; however, the common SDN implementations designed for wired networks are not directly amenable to the distributed, ad hoc, low-power, mesh networks commonly found in IoT systems. SDN promises to improve the overall lifespan and performance of IoT networks. However, the SDN architecture changes the IoT network's communication patterns, allowing new types of attacks, and necessitating a new approach to securing the IoT network. Black SDN is a novel SDN-based secure networking architecture that secures both the meta-data and the payload within each layer of an IoT communication packet while utilizing the SDN centralized controller as a trusted third party for secure routing and optimized system performance management. We demonstrate through simulation the feasibility of Black SDN in networks where nodes are asleep most of their lives, and specifically examine a Black SDN IoT network based upon the IEEE 802.15.4 LR WPAN (Low Rate - Wireless Personal Area Network) protocol.**

I. Introduction

The Internet of Things (IoT) is pervasively growing around us. IoT refers to a system of smart objects that communicate electronically and may form low power, low duty cycle, ad-hoc, wireless mesh networks. IoT systems are found in healthcare (medical monitoring devices), electrical utilities (smart meters), physical security (wearable or wireless cameras), transportation (smart cars), industrial automation and controls and within large composite systems like Smart Cities. IoT nodes are often powered by a small battery that lasts months to a few years. This energy-efficient operation is possible as the nodes 'sleep' a majority of the time and 'awaken' to transmit small amounts of information. Given the size of these nodes, they have computational, memory, range of operation and energy constraints and must run efficient communication protocols. A widely used communication protocol for IoT is IEEE 802.15.4 LR-WPAN (Low Rate Wireless Personal Area Networks) [2]. 802.15.4 defines the Physical layer and the MAC-sublayer of the Link layer of the communications protocol. The network, transport and application layers are defined by protocols that are built on top of 802.15.4 such as 6LoWPAN [24], ZigBee [1] and WirelessHART [12]. All of these protocols use the nodes as routers to send information to the next hop and on to the final destination. While IoT communication protocols provide basic security functions, these standardized security functions are often not sufficient for IoT nodes that are carrying mission-critical information. Therefore, improved security and reliability of IoT networks is a key requirement for these networks.

IoT networks are growing exponentially (billions of devices today), and will face the same evolutionary security challenges as current IP networks. Furthermore, mission-critical IoT networks must be extremely secure - privacy, confidentiality, integrity and authentication must be designed in from the base protocols on up.

In this paper, we introduce Black Networks to mitigate traffic analysis and data gathering attacks. A Black Network is a network that secures each layer of the communication stack by encrypting all of the meta-data contained within the communication (including the source and the destination addresses), in addition to the payload. We examine the impact of a Black Networks on the routing performance of the network and identify the need for a trusted-third party in order to route efficiently.

We present Black SDN, a secure SDN IoT network architecture that utilizes an SDN controller as the trusted-third party in the Black Network. The primary goal of Black SDN is to secure communications by encrypting the header and the payload at the Network layer to mitigate a range of attacks, including traffic analysis/inference attacks. Header encryption causes routing challenges. We propose a simple broadcast routing, and a more efficient and secure SDN routing An SDN architecture improves IoT network security and efficiency for Black Networks. All approaches must consider asynchronous node 'sleep' and 'wake' cycles. We simulate Black SDN for IoT in star and mesh topologies and evaluate the results.

The major contributions of this paper are: Black Networks, Black broadcast routing, Black Routing with Trusted Third Party (TTP) and SDN as the TTP.

The remainder of this paper is organized as follows: In Section II, we provide an overview of IoT networks and the security of 802.15.4 protocols. In Section III we present Black Networks, the basis for Black SDN, a method of securing IoT networks for privacy, confidentiality, integrity and authentication, at the Link Layer and Network Layer, and its resulting routing challenges. We present Black SDN for IoT networks in Section IV. We evaluate the security of Black SDN in Section V and analyze the results of our simulations. We draw the relevant conclusions and suggest future areas of research in Section VI.

II. IoT Networks Security Overview

In this subsection, we provide a security overview for IoT protocols. The IEEE 802.15.4 standard defines the Physical layer (PHY) and the Link layer (Link) in the communication stack while protocols like 6LowPAN, ZigBee and WirelessHART define the Network, Transport and some of the Application layers. We review the security services at each layer.

978-1-4673-9101-6/15 $31.00 © 2015 IEEE
DOI 10.1109/MASS.2015.100

A. Security Introduction

There are several fundamental security services in a simple IoT communication protocol: *access control/authentication, message integrity, message confidentiality, and replay protection.* These security services provide a basic level of protection and, ideally, are provided at each layer in the communication protocol stack. Higher layer protocols should provide additional security services, such as *routing integrity* and *routing assurance* which should be provided at the Network layer, and *application security* at the Application Layer.

These basic security services do not protect against all potential attacks. A range of attacks are still possible including track and trace, node capture and higher layer attacks such as selective node forwarding. Furthermore, attacks on the meta-data associated with each frame and packet can be used for a broad range of attacks such as an inference attack, traffic analysis, a dictionary attack or for eavesdropping, packet injection and packet modification. A detailed review of IEEE 802.15.4 security is presented by Sastry and Wagner [31].

The main security challenges presented by IoT networks are low computational resources, small memory resources, limited physical protections and limited power on the IoT connected smart objects. Power depletion attacks, where a device is forced to utilize all of its available energy to manage malicious communications or perform activities requested by an adversary, require explicit power management services in order to limit the consequences of the attack. Power depletion attacks have created specific security guidelines that are normally not considered in standard networks [36]. Node capture is a practical attack in many IoT deployments due to direct physical access to the devices. Node capture refers to an adversary directly accessing the device, either through physical access or electronic access, allowing the adversary to extract keys, inject messages, operate as an authenticated node and remove nodes from the network. Node capture can be mitigated by enforcing certain security requirements such as erasing secure key information when the node is disassociated from a network [27]. Table I reviews threats and mitigations of each layer in IEEE 802.15.4-based networks [30].

TABLE I. THREATS AND MECHANISMS WITHIN COMMUNICATION LAYERS OF IEEE 802.15.4-BASED PROTOCOLS.

IEEE 802.15.4 Protocol Threats and Mitigation		
Layers	*Threats*	*Mitigation*
Physical	Jamming	Spread Spectrum, Priority Messages, Lower Duty Cycle, Region Mapping, Mode Change
	Tampering	Tamper-proof, hiding
Link	Collision	Error Correcting Code
	Unfairness	Small Frames
	Exhaustion	Rate Limitation
	Replay	Frame Counter
	Meta-data attacks	None
Network	Neglect, Greed	Redundancy, probing
	Homing	Encryption
	Misdirection	Egress Filtering, Authorization Monitoring
	Traffic Analysis	Encryption
	Black Holes	Authorization, Monitoring, Redundancy
	Meta-data attacks	None

B. IEEE 802.15.4 Security

In IEEE 802.15.4, security services are provided by the MAC-sublayer of the Link layer. The security services provided by IEEE 802.15.4 are data authenticity, data confidentiality and replay protection. The MAC PIB (PAN Information Base) maintains a device table that allows authenticated devices to communicate and set the security level between them. Security is requested by the upper layers [40] [31]. The encryption scheme supported by IEEE 802.15.4 is AES-CCM* [2][31][15].

The main threats to this protocol are NO encrypted ACK frames, NO timed frame counters and NULL security level. When the ACK frame is NOT encrypted, an intruder can intercept a MAC frame, forge an ACK frame with a sequence number, resulting in frame loss with no retransmission. Replay attacks send a large number of intercepted frames, with large counters. Valid frames with smaller counters are then rejected by the security mechanisms which do not evaluate based on time-stamps. Unless requested by the higher layers, there is no default security for IEEE 802.15.4. This could result in insecure and compromised systems using IEEE 802.15.4. A detailed review of IEEE 802.15.4 security is presented by Sastry and Wagner [31].

C. 6LoWPAN

6LoWPAN is defined in a collection of IETF standards that define the use of IPv6 for low power WPANs (IETF RFC 4919[24], RFC 6282[13], RFC 6775 and RFC 6550[34]). It uses the PHY and MAC sublayer of IEEE 802.15.4. The large address space of IPv6, and the widespread use of IP allow 6LoWPAN to make smart objects directly addressable to an IP network. 6loWPAN has deployments in automation, control and energy sectors [37][33].

6LoWPAN uses the IPSec security architecture. Park et.al. [27] refer to a set of security considerations for 6LoWPAN. They include efficient adaptation of network layer security for 6LoWPAN including authentication and key management. IPv6 network layer security (IPSec) is resource-intensive to small devices and cannot be directly applied to 6LoWPAN. Internet key exchange (IKEv2) messaging (RFC5996) has a high signaling cost for low power, low data rate devices. Efficient key management and distribution algorithms will have to be defined for 6LoWPAN. Standard IP network threats remain for 6LoWPAN such as DoS, intrusion, sinkhole, replay and insecure routing attacks. To mitigate IPSec vulnerabilities, a combination of Application Level Security SSL, with link layer security IEEE 802.15.4 MAC is recommended. IPSec is not mandated for 6LoWPAN.

D. ZigBee

Zigbee is a set of application protocols, based on the IEEE 802.15.4 PHY and MAC sublayer. ZigBee application profiles form energy-efficient, low data-rate and self-configuring mesh networks of up to 2^{16} devices, using Zigbee devices which are RFD (Reduced Function Devices) or FFD (Full Function

Devices). The Zigbee alliance hosts the multiple Zigbee specifications, standards, member companies and Zigbee device certifications (http://www.zigbee.org). ZigBee has been deployed in a wide variety of consumer electronics, industrial, control, lighting, home, telecom, healthcare and energy segments.

The security architecture of ZigBee has certain architectural guidelines, sublayer interfaces, key definitions and usage models. The security services for the ZigBee protocol is provided by the Security Service Provider, and specified in the Security Services Specification within the ZigBee standard. Services include key establishment, key transport, frame protection and device management.

Fundamental to the ZigBee security architecture is a trusted third party (TTP), called the Trust Center (TC). All ZigBee devices know and trust the TC, and there is only one TC per network. The TC performs network management, configuration management, and the storage and distribution of keys. The centralized ZigBee Trust Center (TC) that generates and updates keys for all devices within the network is a vulnerability. Additionally, when a node disassociates from the network, it still contains the network key (NK), and creates a vulnerability.

E. WirelessHART

WirelessHART is a robust, time synchronized, self-organizing, self-healing, mesh networking protocol, using the IEEE 802.15.4 PHY layer. The TDMA-based MAC sublayer is defined in the WirelessHART standard using TSMP (time synchronized mesh protocol) technology. WirelessHART is primarily used for process control and measurement environments, because of its backward compatibility to the widely-deployed, industrial HART protocol. Industrial control environments require deterministic timing and often have harsh radio interference. WirelessHART is the IEC 62591 standard, and it operates on the 2.4GHz ISM band with 16 channels. Physical layer security on the radio layer consists of Frequency Hopping Spread Spectrum (FHSS) across 16 channels. Clear Channel Assessment (CCA) is optional to determine channel efficiency and configure transmit power levels. *Channel Blacklisting* is a mechanism to disallow the use of rogue channels (channels with interference) [20]. For reliability and redundancy, the WirelessHART mesh network provides routing mechanisms to bypass link failure, interference and inoperative devices - any or all of which could be a result of a malicious attack. Each device is a router and connects to two other devices for path diversity. WirelessHART is designed to be a robust, reliable protocol providing greater than 99.73% availability, but there are limitations with the security architecture. The WirelessHART Security Manager provides security keys generation and management (storage, renewal, revocation). Security keys are not well-defined in the WirelessHART standard [35] [16]. The Security Manager specifications and architecture are not defined in the WirelessHART standard. Along with that, key management definitions are incomplete (only key distribution is defined). This may lead to a compliant, but insecure, implementation. There is an exhaustive threat analysis for WirelessHART by [29].

Resource exhaustion may occur by frequent link scheduling and routing. The 10ms active time slot in WirelessHART limits any continuous resource drain.

We have reviewed the security features for IEEE 802.15.4, 6LoWPAN, ZigBee and WirelessHART, and their challenges.

In all of the above protocols, meta-data, including source and destination addresses are sent in the clear between nodes. This provides for a range of attacks based upon eavesdropping and packet injection attacks. While the IoT nodes are limited in their communication range do to radiated power and receive sensitivity, attackers are not limited in either, allowing for eavesdroppers to operate at more than ten times the maximum communication range between IoT nodes. Thus, there is still a significant need to protect the meta-data within communication packets.

III. Black Networks for IoT

In this section, we present Black Networks for IoT devices. Black Networks secure the meta-data and the payload within each layer. We specifically examine the IEEE 802.15.4 protocol in this section. The Black Network for the 802.15.4 Link layer communications by encrypting the meta-data, and includes the cipher's initialization vector (IV) and encrypted meta-data in the communicated frame. We similarly secure the meta-data independently within the Network layer for protocols such as 6LowPAN, ZigBee and WirelessHART. The resulting 802.15.4 compatible frame, allows the intended recipient to correctly receive and decode the message while all other receiving nodes are unable to decode any data, including the sender and the receiver addresses.

With large networks of IoT nodes, routing becomes critical. We examine the impact of broadcast routing on the performance of Black Networks.

Black Networks mitigate a broad range of both passive and active attacks, due to the authenticated and secured communications at both the Link layer and the Network layer. Adversaries should not be able to determine the source, the destination, the frame sequence number or the replay counter [10].

Location information and communication patterns can be obtained from the meta-data. Prior work in this area has been done by Conti et. al. [5], in wireless sensor networks. Source Location Privacy (SLP) allows the sender location to be hidden from adversaries. SLP is achieved via multiple methods: Random Walk, Geographic routing and Network Layer Anonymity. Some secure routing mechanisms are Random Routing Scheme, Dummy Packet Injection Scheme and Anonymous Communication Scheme (ACS) [22], Anonymous Path Routing (APR) [14], Simple Anonymity Scheme [23], Destination Controlled Anonymous Routing Protocol for Sensor nets (DCARPS) [26] and Hashing Based Identity Randomization [11].

A. Black 802.15.4

1) Black 802.15.4 Link Layer Frame: Figure 1 shows the IEEE 802.15.4 Link layer frame and its transformation to the Black Link Layer frame.

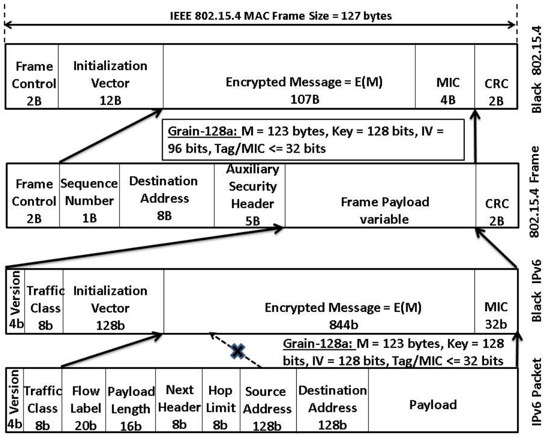

IEEE 802.15.4 MAC Frame Size = 127 bytes
Frame Control 2B
Initialization Vector 12B
Encrypted Message = E(M) 107B
MIC 4B
CRC 2B
Black 802.15.4
Grain-128a: M = 123 bytes, Key = 128 bits, IV = 96 bits, Tag/MIC <= 32 bits
Frame Control 2B
Sequence Number 1B
Destination Address 8B
Auxiliary Security Header 5B
Frame Payload variable
CRC 2B
802.15.4 Frame
Version 4b
Traffic Class 8b
Initialization Vector 128b
Encrypted Message = E(M) 844b
MIC 32b
Black IPv6
Grain-128a: M = 123 bytes, Key = 128 bits, IV = 128 bits, Tag/MIC <= 32 bits
Version 4b
Traffic Class 8b
Flow Label 20b
Payload Length 16b
Next Header 8b
Hop Limit 8b
Source Address 128b
Destination Address 128b
Payload
IPv6 Packet

Fig. 1. IEEE 802.15.4 encryption to Black packet and Black frame

Flags are used to indicate a Black Link layer frame. This is the only meta-data field left unencrypted. The Frame Control field is set to indicate a Black frame for IEEE 802.15.4. The initialization vector (IV) is used to synchronize the cryptographic engines for Link layer communication. Symmetric Link layer keys are used for secure communication and authentication. The IEEE 802.15.4 Black Link layer frame can be formed by encrypting the header and payload as a single block, using the Grain-128a authenticating cipher [3], resulting in an IEEE 802.15.4 compatible frame.

2) Black Network Layer Packet: Figure 1 shows an IPv6 packet transformation into a Black packet. This is usable to maintain privacy and security [24]. The IV replaces the Source and Destination address bits and is expanded to 128 bits. The Traffic Class bits indicate the Black Network layer packet, and Grain-128a is used to encrypt the remainder of the payload and header. A symmetric key is shared between sender and receiver before communication begins. Flow label, payload length, next header, hop limit and destination address are encrypted along with payload and included as the Encrypted Message.

B. Black Network Broadcast Routing Simulation

We examine the impact of a Black Network layer on the routing performance of the network. We specifically examine broadcast routing that mitigates an adversary from determining the destination. We simulate various topologies, explore the use of spanning trees and wake timing to transfer data, under the assumption that all nodes sleep a percentage of time. With large networks, messages are communicated point-to-point between nodes, using a store and forward routing approach at the Network layer.

1) Black Network Simulator: The Black Network Simulator simulates network performance for various topologies and sleep patterns, and implements the functionality for the Network Layer. The simulator investigates broadcast routing in Black Networks, where meta-data, including sender and receiver information, is encrypted. The Black Network Simulator has been designed specifically for generating bounded, random sleep/wake cycles.

2) Packet Functionality: Each Black packet is assigned a Time to Live (TTL) value. This can be a value such as number of hops or an amount of time. Upon reaching the end of TTL, a packet expires and is no longer valid.

3) Node Functionality: IoT devices are simulated as 'Nodes'. Each node has a Node ID and connected to one or more nodes. Every node has a list of nodes that are connected to it. To simulate sleep patterns, each node is in a wake or sleep mode. Nodes sleep and wake, in random patterns, for random time periods. Each node has Packet Memory Buffer, to store Packet IDs of previously broadcast packets. When a packet arrives, its Packet ID is checked against the packet memory buffer, and if present, the packet is not rebroadcast. If the Packet ID is not present, then packet is broadcast and Packet ID is added to packet memory buffer. The buffer size of the packet memory buffer is assumed to be large enough, so that a packet is never retransmitted by a node. When a Black packet arrives at a non-destination node, it is simply rebroadcast. However, when a Black packet reaches the intended recipient (sharing a secret key), the packet is still broadcast, to mask the recipient.

4) Simulated Network Topologies: We simulate the routing of Black packets over multiple network topologies. Node coverage is the number of nodes a Black packet can reach at a certain point in time, when routing through awake nodes. Each topology has a 100% node coverage when all nodes are awake. Node coverage is measured for sleep percentages from 0% to a 100% at regular sleep intervals. The standard deviation for ten thousand iterations is the final node coverage for a sleep percentage. We run our simulation over the following topologies, of a 100 nodes:

- *Fully-connected mesh* is the baseline topology. All awake nodes receive the Black packet since the distance between any two nodes is 1-hop, regardless of the number of asleep nodes.
- *Varied star* example (with 20 nodes) is shown in Figure 2. Any node is reachable only through the center node.
- *Ring* topology consists of nodes in a circle. Each node has two neighbors. When any two nodes are asleep, nodes in between the sleeping nodes cannot communicate with the rest of the network.
- *Line* topology has each node with two neighbors excepting the first and the last nodes. When a node sleeps, connectivity between all the nodes on either sides of sleeping node is severed.
- *Star* topology has a central node and five lines of nodes attached to it. A node on any arm of the star can be reached only through the central node.
- *Random-connected mesh* topology has each node connected to a random number of nodes. Each node may connect from one to a hundred nodes.

C. Simulation Results and Analysis

Simulating the above network topologies, the node coverage is plotted against network performance when a certain percentage of nodes are asleep. In the ideal scenario, all awake nodes

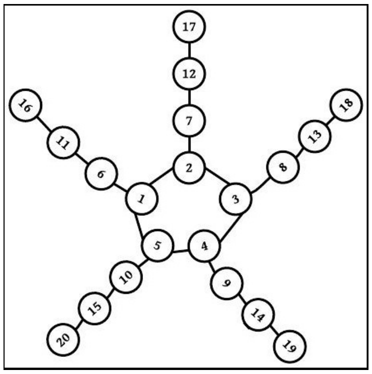


Fig. 2. Varied-Star Network Topology.

should be able to receive a packet, when a certain percent of nodes are asleep. From Figure 3 we observe that the fully connected mesh topology is closest to the ideal scenario. For the other topologies, there is a steep drop in the node coverage when just 10% of nodes are asleep. The network efficiency is at an average of 30% when nodes are asleep only 10% of the time.

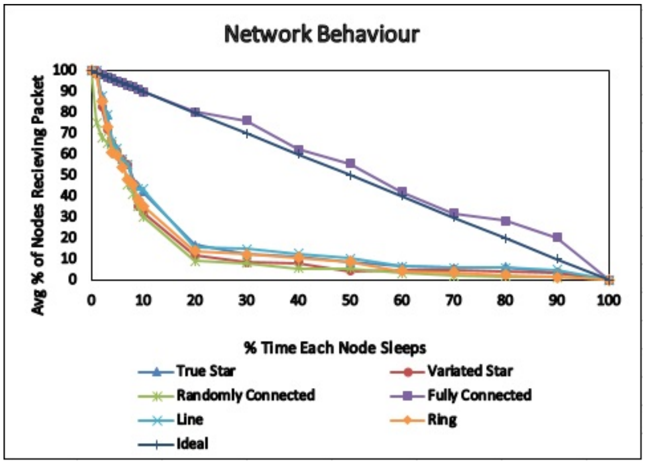


Fig. 3. Simulation results for broadcast routing with randomly sleeping nodes

This steep drop is a result of the nodes in the critical path between sender and receiver (e.g. the center node(s) in a star topology), are asleep and nodes connected to them are unreachable, even if they are awake.

The simulated results affirm that a broadcast routing is not very efficient in IoT networks, for most network topologies. Implementing a fully connected mesh topology is resource-intensive and impractical even with a small number of nodes. A routing protocol providing adequate node coverage without sacrificing security, integrity and confidentiality needs to be established. An approach that needs to be evaluated is store and forward - a node stores the packet when it's neighbor is asleep and delivers it once it awakens. Additionally, a control signal that wakes up a critical node long enough to broadcast also needs to be investigated. The broadcast protocol, while effective in eliminating possibility of an internal node discovering sender or receiver, it is not very efficient in node coverage. The simulator currently measures performance by calculating standard deviation of node coverage. Broadcast throughput has to be measured accurately, given that a significant portion of the bandwidth is utilized by the packets that route till end of TTL, and are not in the path to reach the destination.

In sensor networks, nodes are mobile, establishing and severing connections between each other. Selected nodes can be established as Trusted Nodes that keep track of the location and, perhaps, include directionality while broadcasting. Another possibility is to multi-cast instead of broadcast, and also have trusted nodes assigned a partial key so that they know the direction of the destination and might also edit the TTL of a packet accordingly. Also, when the receiving node broadcasts, the TTL can be set to a minimum value for efficient bandwidth use.

D. SDN Controller: The Need for a Trusted Third Party

In Section II, we outline the security challenges, and vulnerabilities for IoT communication protocols - 802.15.4, 6LoWPAN, ZigBee and WirelessHART. SDN networks and the OpenFlow protocol [17] have similar challenges for IoT networks. We note that security contributions in the emerging field of SDN IoT networks are limited. In this section, we motivate and define the open problem of security for SDN IoT networks.

The general security problem we are addressing is: How does a packet get from node A to node B without an eavesdropper knowing that the packet went to node B?

The specific problem we are attempting to solve is: How does a packet get from node A to node B, *in an IoT network*, without an eavesdropper knowing that the packet went to node B? This translates to incorporating privacy within IoT network communications.

We resolve the privacy problem in Section III through Black Networks - where the data and the meta-data of the frame, and packet, are secured at the Link and Network layers. This, however, presented a routing challenge in IoT networks, for peer-peer data transfer, where a packet may not reach its destination, if the intermediate nodes were asleep a majority of the time (which is a practical scenario).

The goal is to resolve the routing problem, with Black packets, in IoT networks. This means getting a Black packet from Node A to Node B, with intermediate nodes on their configured 'sleep'/'wake' schedule. The solution would have the added benefit of incorporating confidentiality, integrity and authentication for all communications. Additionally, it would mitigate a host of inference, traffic analysis, power depletion attacks and packet length-based attacks. As declared, it is not sufficient to receive the Black packet at its final destination, but also necessary to ensure that the receiving node (Node B) is unknown to an external observer.

We further outline our assumptions associated with the problem definition of routing in Black networks. They are:

- The operating environment is an IoT network consisting of low-power resource-constrained nodes in a mesh configuration. Heavy-duty protocols (such as IPsec, SSL/TLS) cannot be supported in this environment.
- When a node transmits, it is known. An external observer knows who transmitted data.
- A trusted third party (TTP) exists in the network, as an anchor, with a network topology view.
- Nodes operate in synchronous or asynchronous modes.
- TTP and nodes communicate via shared secret key

In Section IV, we present a solution for our problem definition with the above assumptions.

IV. Black SDN for IoT Networks

Software Defined Networking (SDN) has been proposed to streamline network architecture, complexity and scalability [19]. SDN separates the control plane (signaling) from the data plane (media) in an IP network [9] [25], resulting in a scalable and very cost effective architecture. The routers (now called forwarding elements or switches) have minimal logic to forward data (and can be simple compute elements, without complex, expensive routing logic). The forwarding decisions are based on Flow Tables that are downloaded to the nodes by a centralized SDN controller, with a global network view. The controller communicates with the switches using an open, industry-defined, protocol called OpenFlow [4]. All other functions - protocols, middle-box functionality and network management and configuration reside in the SDN controller SDN security has been a major concern for potential adoptees. SDN security vulnerabilities are assessed to be within the seven areas in the network [18]. The OpenFlow standard describes basic TLS for controller-node security, but does not mandate it [32]. TLS, even with certificate-based authority, has well-known vulnerabilities. All of the scenarios have been proposed for large, broadband IP networks (enterprise, data centers and service providers).

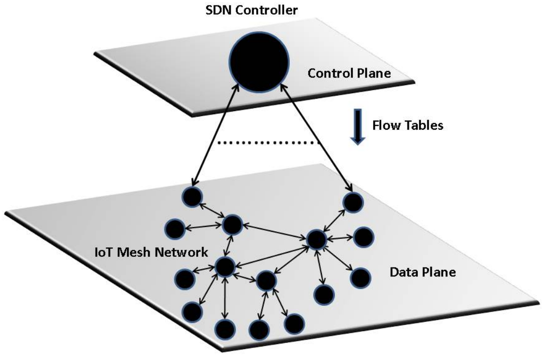


Fig. 4. IoT Network with an SDN Controller

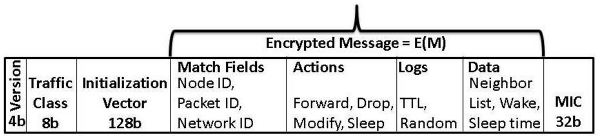
IoT networks with an SDN architecture (Figure 4) have to contend with additional vulnerabilities of resource-constrained nodes, operating in a low-power WSN environment, with all the vulnerabilities outlined in Section II. SDN for IoT is an architectural approach that incorporates an SDN controller in an IoT network. Resource-constrained IoT nodes cannot support a full SDN implementation - reserved for large, complex, broadband, IP networks. Adaptations of the SDN controller for IoT networks have been presented in [38] [6] [21][39].

An architecture for SDN design to WSNs based on 802.15.4, with a simple flow table description, duty cycle handling and in-network data aggregation has been presented in [6]. An SDN protocol for WSNs, Sensor OpenFlow, based on the OpenFlow standard is presented by [21]. Sensor Openflow addresses some of the challenges with SDN applied to IoT such as in-situ data aggregation, simplicity of the flow tables, control plane communication between controller and forwarding element and minimizing the overhead of control channel traffic. Both of these approaches consider a simple network with a single controller. However, [39], proposes SDN architecture for IoT networks within a complex domain (like smart cities), which has multiple IoT networks running heterogeneous mobile technologies. The resulting UbiFlow controller maintains partitions across multiple controllers to load-balance, guarantee performance, manage scalability and mobility. An SDN architecture for IoT, for heterogenous wireless networks with different classes of IoT traffic, on a single, layered IoT SDN controller is presented in [28].

The above SDN for IoT architectures and implementations have not focused on security. SDN for IoT security challenges are a combination of SDN, IoT and network security vulnerabilities. The security for SDN IoT networks are rudimentary and nascent, and highly secure SDN IoT Networks remains an open problem as defined in Section III-D. In this section we present a highly secure Black SDN for IoT networks. This secure IoT network is enabled via an SDN controller (adapted for WSNs), and results in superior network performance, security and payload efficiency in star and mesh networks. We compare the results with non-SDN IoT networks.

The Black SDN for IoT consists of a star, or mesh, wireless IoT network that communicates with an IoT-adapted SDN controller. The SDN controller and the IoT nodes communicate via Black packets (III). An example of an SDN controller to IoT node *control* Black packet is shown in Figure 5. The fields are aligned for header fields, actions and logs/counters. Control Black packets from the IoT node to the SDN controller are identical in format. Header match fields could be Packet ID, Node ID and/or Network ID. The standard actions to act on a Black packet would be Forward, Drop, Modify (the data within the packet) or Sleep (for a given time period). The logs would include TTL (time-to-live) and Random (a small random value to forward Black packets, or rebroadcast them, to obfuscate the receiver). The Data field would contain neighbor lists, wake/sleep times and other parameters.

Using these minimal set of control parameters, we present and simulate three scenarios across topology (star or mesh), synchronization (synchronous or asynchronous) and transmission mode (broadcast or routing). In each case, we evaluate if the SDN controller is more effective for routing and security.



			Encrypted Message = E(M)				
Version	Traffic Class	Initialization Vector	Match Fields	Actions	Logs	Data	MIC
4b	8b	128b	Node ID, Packet ID, Network ID	Forward, Drop, Modify, Sleep	TTL, Random	Neighbor List, Wake, Sleep time	32b

Fig. 5. Black SDN for IoT Control Packet example

A. Scenario 1 - Broadcast on Star Network

Topology=Star, Sync = Y, Broadcast = Y, Controller = Y In this star topology, all nodes sleep and awake at the same time (are in sync), based on a controller initiated sleep/wake schedule and absolute time (clock). This is refreshed on a regular basis to eliminate timing drifts in the system. Assuming nodes are only within radio reach of controller (and not each other), inter-nodal communication occurs via SDN controller. Sending node broadcasts to controller, which in turn broadcasts to all nodes, including destination node. This ensures that the destination is obfuscated to an eavesdropper, even if the source is known (it is assumed that the transmitting source is known to an attacker). All nodes may re-broadcast the packet to further confuse the attacker as to whether the packet was accepted or rejected by receiver. In this scenario, the controller acts as a gateway.

If the nodes are within radio reach of each other, then a controller is not necessary. Nodes broadcast to each other, and then re-broadcast to mask the destination.

It must be noted that the overall system may not be secure for a small number of nodes (which is typical in a star network), and a statistical inference can be made on source and destination.

B. Scenario 2 - Synchronized Mesh Network

Topology=Mesh, Sync = Y, Route = Y, Controller = Y Like Scenario 1, in this mesh network all nodes are in controller-managed sync. The originator node, requests a route from the SDN controller, when it has to transmit. The SDN controller maps a route downloads flow tables to the transmitting node and intermediate nodes. When nodes are in the wake cycle, the Black packet gets transmitted per hop.

The other option for routing the Black packet is via an onion router method [8] [7]. In this case, the SDN controller dynamically determines the next hop for the Black packet. At every wake cycle, the SDN controller having dynamically determined the next hop, downloads it to the current node storing the Black packet. This method is more secure and reliable than setting up an end-to-end path ahead of time. It also has a higher performance impact due to the control traffic generated during every wake cycle to all nodes (again to mask destination).

Figure 6 shows the simulated results of Black packet latency for Scenario 2, for a network path with upto 10 hops. Sleep times range from 0.5 ms to 10ms (approximately upto 95% sleep cycle).

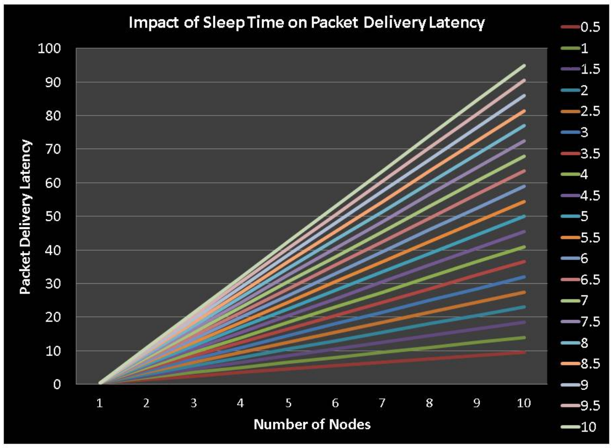


Fig. 6. Scenario 2: Black SDN Packet Latency

C. Scenario 3 - Unsynchronized Mesh Networks

Topology=Mesh, Sync = N, Route = Y, Controller = Y Scenario 3 is the most challenging of all the scenarios. Sleep and wake cycles for the IoT nodes are not synchronized. Consequently, some nodes are asleep, while others are awake, in no particular order. Black packets transmitted to nodes that are sleeping, do not reach them. Consider Node A sending a Black packet to Node B. In this case, the SDN controller, based on its network map, downloads routes to the subset of nodes, that are adjacent to Node A and whose wake times overlap with Node A. Node A broadcasts the Black packet to these nodes and the process repeats until destination Node B. It is possible that NONE of Node A's adjacent nodes are awake during A's wake cycle. In which case, the SDN controller instructs Node A to sleep until the next hop awakes, and then the Black packet is transmitted. To eliminate such conditions, during operation, IoT network configurations should be managed accordingly. Node join requests must be initially populated with proper asymmetric cycle times, such that adjacent nodes have adequate overlapping awake times. This IoT network configuration should be done at the start when the nodes are joining the network. Figure 7 shows the simulated results of Black packet latency for Scenario 3, for a network path with upto 10 hops. Sleep times range from 1ms to 10ms. (approximately upto 90% sleep cycle, for asynchronous networks).

V. Evaluation and Analysis

Our motivation for presenting Black SDN for an IoT network is aimed towards enhanced security and network performance for mission-critical networks.

1) Network Performance: In Section III we provide an extensive analysis of broadcast routing for Black Networks over multiple network topologies. Black Networks provide for a secure approach to communication by protecting each layer in the communication hierarchy - at at the expense

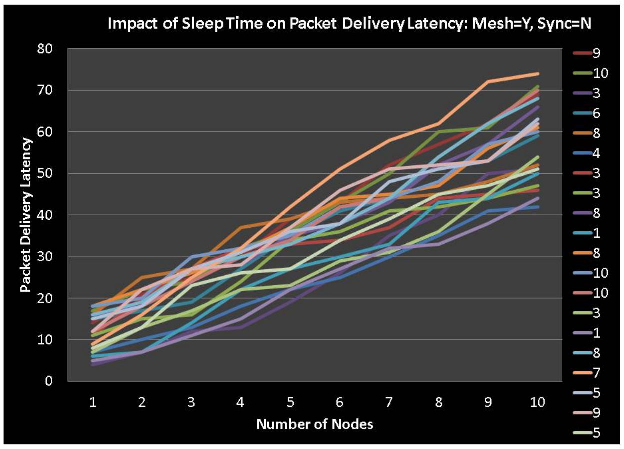


Fig. 7. Scenario 2: Black SDN Packet Latency

of complicating the routing through the network. Simple broadcast provides for the most secure routing approach, but it consumes significant energy across all nodes in the network. Furthermore, the network topology has a significant impact on the success of broadcast routing. Equal length paths between two nodes increase the likelihood of collisions, and limited numbers of paths between two nodes makes the network susceptible to becoming disjoint with both collisions and the use of sleep modes. Comparing with the Black SDN for IoT - we show that network performance is markedly better, as the SDN controller maintains the state of the network and its components. Black packet delivery - through either synchronization and sleep, reach their final destination, with latency, when nodes sleep a majority of the time. We note this for the star and the mesh topologies. One area of concern for Black SDN for IoT is the generation of control traffic as a result of increased communication between the SDN controller and the IoT nodes. Further, the need to maintain anonymity results in additional messages being sent to obscure the recipient of the message. There is increased control messaging between SDN controller to IoT, for Scenario 2 (synchronous mesh), as the nodes wake and sleep at the same time. The possibility of message storms and the capacity handling ability of the SDN controller are areas of concern. With Scenario 3 (asynchronous mesh), the control messaging is lower, at the cost of increased latency in packet delivery.

2) Security: Black SDN provides a higher level of security than existing 802.15.4 protocols. Black SDN for IoT provides confidentiality, integrity, authentication and privacy. Table II compares the payload efficiency of IEEE 802.15.4 Link layer frame with an implicit nonce (nonce constructed out of header fields), to a Black frame. Black frames provide Privacy, Confidentiality, Integrity and Authenticity, by encrypting the header and 93 byte payload. We note that at higher IEEE 802.15.4 security levels (when both encryption and authentication are applied to the payload), Black frames provide equivalent, or better, payload capacities with a higher level of security (6% better vs. ENC-MIC-64 and 16% better vs. ENC-MIC-128). Unlike Black frames, the IEEE 802.15.4 options of no security, authentication only, and encryption only can lead to insecure implementations susceptible to a range of attacks as shown in Table I. While inference attacks can be made on the 802.15.4 variable payload, the Black frame mitigates payload length-based attacks because of its fixed size.

TABLE II. PAYLOAD EFFICIENCY OF BLACK FRAME.

Comparison of 802.15.4 Link layer with Black Frame		
Security Level	*802.15.4 Payload*	*Black Payload*
No Security	114 bytes	93 bytes
ENC-MIC-32	92 bytes	93 bytes
ENC-MIC-64	88 bytes	93 bytes
ENC-MIC-128	80 bytes	93 bytes
Encryption only	96 bytes	93 bytes

VI. Conclusions and Future Research

Black SDN for IoT enables a secure Internet of Things. The Internet of Things will continue to grow and encompass all aspects of our lives. IEEE 802.15.4-based IoT devices will continue to play a significant part in IoT expansion. IoT devices are engaged in mission-critical functions in multiple industries. Current IoT protocols are vulnerable to a range of attacks including eavesdropping and packet injection attacks based upon the plain text meta-data. Securing the communications between IoT devices, by encrypting both the data and the meta-data, at the Link and Network layers prevents an additional range of attacks including eavesdropping, track and trace, packet injection, and packet modification attacks. A Black Network method of securing all data, provides for high security within a network, at the expense of symmetric key management, decreased network efficiency, and complicated routing. As networking paradigms shift to embrace Software Defined Networking (SDN) in enterprises and Service Providers, IoT networks will utilize the architecture to form the basis for a secure Internet of Things.

Simple broadcast provides for the most secure routing approach, but it consumes significant energy across all nodes in the network. Furthermore, the network topology has a significant impact on the success of broadcast routing. Equal length paths between two nodes increase the likelyhood of collisions, and limited numbers of paths between two nodes makes the network susceptible to becoming disjoint with both collisions and the use of sleep modes.

Future areas of research in Black Networks will focus on better routing mechanisms. These include developing sleep synchronization protocols that are appropriate for Black Networks in order to ensure packet delivery to all nodes. They also include routing for energy-efficient IoT nodes to minimize resource usage. Obfuscating the transmitting source, is an open problem for IoT network security. Another area of future research is to secure the Black Link layer frame by multiple methods that would allow for a fine-grain approach to securing the meta-data such as, *a)* replacing the meta-data fields by Grain-128a IV and a keystream, or *b)* using the AES-EAX mode and *c)* using a pre-shared IV to allow for better payload efficiency. Finally, extending Black Networks to non-IoT networks is needed, along with a standards initiative for secure IoT networks.

References

[1] "ZigBee Specification (January 2008), Zigbee document 053474r17. Technical report.

[2] IEEE Standard for Local and metropolitan area networks Part 15.4: Low-Rate Wireless Personal Area Networks (LR-WPANs). IEEE Standards Association, IEEE Computer Society, June 2011.

[3] M. Ågren, M. Hell, T. Johansson, and W. Meier. Grain-128a: A new version of Grain-128 with optional authentication. *International Journal of Wireless and Mobile Computing*, 5(1):48–59, 2011.

[4] O. S. Consortium et al. Openflow switch specification version 1.0. 0, 2009.

[5] M. Conti, J. Willemsen, and B. Crispo. Providing Source Location Privacy in Wireless Sensor Networks: A Survey. *Communications Surveys Tutorials, IEEE*, 15(3):1238–1280, Third 2013.

[6] S. Costanzo, L. Galluccio, G. Morabito, and S. Palazzo. Software Defined Wireless Networks: Unbridling SDNs. In *Software Defined Networking (EWSDN), 2012 European Workshop on*, pages 1–6. IEEE, 2012.

[7] R. Dingledine, N. Mathewson, and P. Syverson. Tor: The second-generation onion router. Technical report, DTIC Document, 2004.

[8] D. Goldschlag, M. Reed, and P. Syverson. Onion routing. *Communications of the ACM*, 42(2):39–41, 1999.

[9] P. Goransson and C. Black. *Software Defined Networks: A Comprehensive Approach*. Elsevier, 2014.

[10] B. Greenstein, D. McCoy, J. Pang, T. Kohno, S. Seshan, and D. Wetherall. Improving wireless privacy with an identifier-free link layer protocol. In *Proceedings of the 6th international conference on Mobile systems, applications, and services*, pages 40–53. ACM, 2008.

[11] L. Grieco, G. Boggia, S. Sicari, and P. Colombo. Secure wireless multimedia sensor networks: A survey. In *Mobile Ubiquitous Computing, Systems, Services and Technologies, 2009. UBICOMM '09. Third International Conference on*, pages 194–201, Oct 2009.

[12] HARTcomm.org. Wirelesshart [online]. http://en.hartcomm.org.

[13] P. T. J. Hui. Compression Format for IPv6 Datagrams over IEEE 802.15.4-Based Networks. RFC 6282, RFC Editor, September 2011.

[14] J. Jiang, J. Sheu, C. Tu, and J. Wu. An Anonymous Path Routing (APR) Protocol for Wireless Sensor Networks. *Journal of Information Science and Engineering*, 27(2):657–680, 2011.

[15] J. Jonsson. On the security of CTR+ CBC-MAC. In *selected Areas in Cryptography*, pages 76–93. Springer, 2003.

[16] A. N. Kim, F. Hekland, S. Petersen, and P. Doyle. When HART goes wireless: Understanding and implementing the WirelessHART standard. In *Emerging Technologies and Factory Automation, 2008. ETFA 2008. IEEE International Conference on*, pages 899–907. IEEE, 2008.

[17] R. Klöti, V. Kotronis, and P. Smith. Openflow: A security analysis. *Proc. Wkshp on Secure Network Protocols (NPSec). IEEE*, 2013.

[18] D. Kreutz, F. Ramos, and P. Verissimo. Towards secure and dependable software-defined networks. In *Proceedings of the second ACM SIGCOMM workshop on Hot topics in software defined networking*, pages 55–60. ACM, 2013.

[19] D. Kreutz, F. M. Ramos, P. Verissimo, C. E. Rothenberg, S. Azodolmolky, and S. Uhlig. Software-defined networking: A comprehensive survey. *proceedings of the IEEE*, 103(1):14–76, 2015.

[20] T. Lennvall, S. Svensson, and F. Hekland. A comparison of WirelessHART and ZigBee for industrial applications. In *IEEE International Workshop on Factory Communication Systems*, volume 2008, pages 85–88, 2008.

[21] T. Luo, H.-P. Tan, and T. Q. Quek. Sensor openflow: Enabling software-defined wireless sensor networks. *Communications Letters, IEEE*, 16(11):1896–1899, 2012.

[22] X. Luo, X. Ji, and M.-S. Park. Location Privacy against Traffic Analysis Attacks in Wireless Sensor Networks. In *Information Science and Applications (ICISA), 2010 International Conference on*, pages 1–6, April 2010.

[23] S. Misra and G. Xue. SAS: A Simple Anonymity Scheme for Clustered Wireless Sensor Networks. In *Communications, 2006. ICC '06. IEEE International Conference on*, volume 8, pages 3414–3419, June 2006.

[24] C. S. N. Kushalnagar, G. Montenegro. IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs): Overview, Assumptions, Problem Statement, and Goals. RFC 4919, RFC Editor, August 2007.

[25] T. D. Nadeau and K. Gray. *SDN: Software Defined Networks*. O'Reilly Media, Inc., 2013.

[26] A. A. Nezhad, A. Miri, and D. Makrakis. Location privacy and anonymity preserving routing for wireless sensor networks. *Computer Networks*, 52(18):3433 – 3452, 2008.

[27] S. Park, K. Kim, W. Haddad, S. Chakrabarti, and J. Laganier. IPv6 over low power WPAN security analysis. Technical report, IETF Internet Draft draft-6lowpan-security-analysis-05, 2011.

[28] Z. Qin, G. Denker, C. Giannelli, P. Bellavista, and N. Venkatasubramanian. A Software Defined Networking Architecture for the Internet-of-Things. In *Network Operations and Management Symposium (NOMS), 2014 IEEE*, pages 1–9. IEEE, 2014.

[29] S. Raza, A. Slabbert, T. Voigt, and K. Landernas. Security considerations for the WirelessHART protocol. In *Emerging Technologies & Factory Automation, 2009. ETFA 2009. IEEE Conference on*, pages 1–8. IEEE, 2009.

[30] S. Saleem, S. Ullah, and K. S. Kwak. A study of IEEE 802.15. 4 security framework for wireless body area networks. *Sensors*, 11(2):1383–1395, 2011.

[31] N. Sastry and D. Wagner. Security considerations for IEEE 802.15. 4 networks. In *Proceedings of the 3rd ACM workshop on Wireless security*, pages 32–42. ACM, 2004.

[32] S. Scott-Hayward, G. O'Callaghan, and S. Sezer. SDN security: A survey. In *Future Networks and Services (SDN4FNS), 2013 IEEE SDN for*, pages 1–7. IEEE, 2013.

[33] Z. Shelby and C. Bormann. *6LoWPAN: The wireless embedded Internet*, volume 43. John Wiley & Sons, 2011.

[34] Z. Shelby, S. Chakrabarti, E. Nordmark, and C. Bormann. Neighbor discovery optimization for IPv6 over low-power wireless personal area networks (6LoWPANs). RFC 6775, RFC Editor, November 2012.

[35] J. Song, S. Han, A. K. Mok, D. Chen, M. Lucas, and M. Nixon. WirelessHART: Applying wireless technology in real-time industrial process control. In *Real-Time and Embedded Technology and Applications Symposium, 2008. RTAS'08. IEEE*, pages 377–386. IEEE, 2008.

[36] F. Stajano and R. Anderson. The resurrecting duckling: security issues for ubiquitous computing. *Computer*, 35(4):22–26, 2002.

[37] P. Thubert, A. Brandt, T. Clausen, J. Hui, R. Kelsey, P. Levis, K. Pister, R. Struik, and J. Vasseur. RPL: IPv6 routing protocol for low power and lossy networks. *IETF draft[Online]. http://tools. ietf. org/html/draft-ietf-roll-rpl-19*, 2011.

[38] Á. L. Valdivieso Caraguay, A. Benito Peral, L. I. Barona López, and L. J. García Villalba. SDN: Evolution and Opportunities in the Development IoT Applications. *International Journal of Distributed Sensor Networks*, 2014, 2014.

[39] D. Wu, D. I. Arkhipov, E. Asmare, Z. Qin, and J. A. McCann. UbiFlow: Mobility Management in Urban-scale Software Defined IoT.

[40] Y. Xiao, H.-H. Chen, B. Sun, R. Wang, and S. Sethi. MAC security and security overhead analysis in the IEEE 802.15. 4 wireless sensor networks. *EURASIP Journal on Wireless Communications and Networking*, 2006, 2006.