ICST Transactions
on Ubiquitous Environments

Research Article ICST.ORG

An Energy-Efficient Technique to Combat DOS Attacks in Delay Tolerant Networks

G. Ansa*, H. Cruickshank and Z. Sun

Centre for Communication Systems Research, University of Surrey, Guildford, United Kingdom

Abstract

Delay tolerant networks (DTN) are highly constrained networking environments low in resources such as memory, bandwidth, battery and processing power. In opportunistic DTNs, nodes cooperatively forward packets for each other through the carry-store-and-forward paradigm. Opportunistic data forwarding can be abused by an adversary by injecting bogus packets in order to waste the resources of the network. To guard against such attacks, it is important to authenticate packets at intermediate nodes. Packet authentication in itself comes with overheads such as computation cost and energy consumption which can be exploited by an attacker to mount denial of service (DOS) attacks. We propose the use of light-weight DTN-cookies to protect this vital security service from such malicious exploitation.

Keywords: Denial of service, attacker, delay tolerant network, resource exhaustion, network performance.

Received on 8 September 2011; accepted on 5 January 2012; published on 29 March 2012

doi: 10.4108/trans.ubienv.2012.e6

1. Introduction

Delay tolerant networking is fast becoming an area of great research interest. Delay Tolerant Networks (DTN) allow nodes to communicate through asynchronous messaging in situations where an end-to-end path does not exist [1]. DTN falls into the category of "Challenged" networks which is characterized by high latency, low data rate, long queuing times, and long periods of disconnection. DTN is an overlay on top of a number of heterogeneous networks including the Internet [2]. It introduces a new protocol layer, the bundle layer which sits on top of the transport layer. The problem of intermittent connectivity is overcome through the carry-store-and-forward message switching technique [3] and the inherent mobility of nodes [4] as shown in Figure 1.

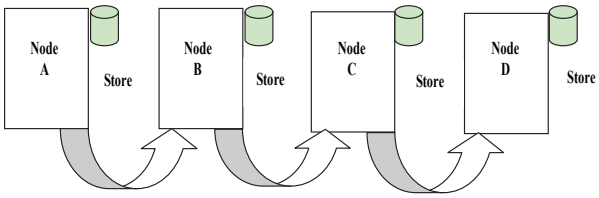

Figure 1. DTN Carry-Store-and-Forward Message Mechanism

At the inception of the DTN concept, a lot of focus was on deep space communications and the Interplanetary Internet. Over the years there has been a steady increase of interest by the research community in the deployment of DTN in terrestrial environments. Examples of DTN terrestrial applications include wild life tracking, providing connectivity to underdeveloped regions, social awareness and pocket-switched-based networks, inter-vehicular and vehicle-infrastructure connectivity and delay tolerant sensor networks [2].

Message delivery in Opportunistic DTNs is dependent on the cooperation of intermediate nodes in accepting

*Corresponding author, Email: g.ansa @surrey.ac.uk

custody of a packet and forwarding same when a node comes into range with another node. Such opportunistic forwarding consumes buffer space and network bandwidth.

To reduce communication overhead especially when multi-copy routing/forwarding is used, packets have to be authenticated [4]. Security is one of the most important but least researched areas in DTN. For DTN to gain wide acceptability and enjoy large-scale deployment, it has to guarantee secure communications to network users.

The three most important security services of any computer system or network are confidentiality, integrity and availability [5], [6]. Confidentiality prevents a non-trusted party from having access to secret data. Data integrity prevents the modification of data while the packet is on transit and the acceptance of replayed packets. Availability ensures that legitimate users are guaranteed access to network resources when requested [7].

Denial of service attacks is a major threat to availability because it prevents a user or network from fulfilling its functions by disabling or degrading the services it provides [5]. The primary goal of DOS attacks is to prevent access to a particular resource [8].

There are two types of DOS attacks that have minimal cost to the attacker: flooding attacks and logic attacks [7]. A flooding DOS attack is based on brute force where a large volume of traffic is sent to overwhelm a victim or target. Buffers are filled; network bandwidth and CPU cycles are wasted on unnecessary processes.

A logic attack on the other hand cleverly exploits vulnerabilities in the target (host, routers, gateways or a protocol). Security mechanisms should be designed in such a way that they do not become vulnerable to Denial of Service (DOS) attacks.

A classification of DOS attacks by the Computer Emergency Readiness Team (CERT) [9] groups DOS into three types: the destruction or alteration of configuration information, physical destruction and alteration of network components and consumption of scarce, limited and non-renewable resources. The main focus of this paper is to protect *"the scarce, limited and non-renewable resources"* from exhaustion.

Designing a DOS resilience mechanism for "Challenged" networks like a DTN requires new techniques. In terrestrial DTN scenarios nodes function as hosts and routers. These nodes can opportunistically and cooperatively forward packets from a source to a destination in a multi-hop scenario. An attacker can use the message forwarding mechanism to exploit the authentication/access control checks by injecting bogus packets into the network.

The aim is to deplete the scare resources of the DTN which include battery power, bandwidth, CPU cycles, communication contact time and memory. This problem is further compounded when multi-copy packet routing/forwarding is adopted to boast the packet delivery ratio.

In this paper, we propose mechanisms to detect and react quickly to this type of DOS attack. Protocol-based DOS attacks are a serious threat to availability. Access control systems most often use strong resource demanding authentication which subjects nodes to resource-intensive operations making them points of congestion.

The focus of this paper is to minimize the impact of security processing on the energy of constrained nodes. The overall objective is to keep computational and communication costs low, reduce latency and prolong the life of the network. The Opportunistic Network Environment (ONE) [10] simulator is used to build the application scenario. The simulation results show a significant improvement in delivery ratio, low latency levels and energy savings. In the simulations, attack packets are dropped at the first hop of encounter.

The remainder of the paper is organized as follows. Section 2 discusses related work on DOS mitigation in DTN and other networks. The attacker model, mobility and routing models, design goals, networking and security requirements and assumptions are described in Section 3. Section 4 gives a detailed description of the proposed security mechanisms. The configuration settings, simulation results and performance evaluation are presented in Section 5. We conclude the paper and present our future work in Section 6.

2. Related Work

In terrestrial networks, a number of schemes have been proposed over the years to combat the DOS problem. Dwork and Noar proposed the client puzzle technique [11], to combat the junk mail problem. The scheme requires a sender to compute a puzzle for every message sent. The cost of the mechanism is negligible for normal users of the system when compared to mass mailers.

The TCP SYN flood mechanism proposed by Juels and Brainard [12], is an extension of the client puzzle idea which tackles connection depletion attacks. Another technique that combats protocol-based DOS attacks is the Internet Security Association and Key Management Protocol (ISAKMP) [9], [13]. It is an anti-clogging technique derived from the PHOTORIS protocol where a client is required to return a server generated cookie. The exchange enables the server to verify the client's claim of presence at an IP address and thwarts spoofing attacks.

Meadows [14] proposed a formal framework for network DOS. The idea is to gradually strengthen the authentication process as the protocol executes by introducing a light authentication phase prior to signature verification. The purpose of the framework is to formalize protocol design and make them more resistant to DOS attacks.

These DOS mitigation schemes are designed for low-delay and well-connected networks, requiring a number of message exchanges to initialize the protocol. The disconnected nature of DTN and the wireless

communication medium makes these schemes impracticable.

A comprehensive survey on DOS attacks and defenses in Wireless Sensor Networks (WSN) is presented in [5] which extend the work of Anthony Wood and John Stankovic [15]. This survey gives an insight into possible DOS attacks in each layer of a WSN protocol stack and how they can be mitigated.

Broadcast authentication is used in wireless sensor networks to prevent attackers masquerading as base stations. µTelsa [16] an efficient broadcast authentication scheme could only achieve delayed authentication which is undesirable for time-sensitive broadcast messages.

A dynamic window scheme to mitigate resource exhaustion DOS attacks in broadcast authentication is proposed in [17]. A node is at liberty to decide whether to forward a message first or to verify it first before forwarding.

Deng et al. [18] proposed the use of one-way hash chain to defend against path-based DOS attacks in sensor networks end-to-end communication.

Research in DTN security has been minimal. One of such pioneering works is the Bundle Security Protocol (BSP) specification [19]. The specification identifies "on-path" and "off-path" DOS attacks as threats which must be considered during the design of any DOS defence mechanism for DTN.

In [20] the authors make a comparison to analyse performance between single and multi-copy packet replication in the presence of attackers and the effects on packet delivery ratio. They use different routing schemes to model packet drop attacks, packet flooding, address spoofing, routing table falsification and counterfeiting of acknowledgements. They conclude that the performance of a DTN without authentication degrades gracefully even when a sizeable number of attackers are present in the network.

Packet dropping and address spoofing are two types of DOS attacks identified in [21] which an attacker can use to degrade network performance or prevent a DTN from functioning. The authors propose three protection mechanisms (Opportunistic Protection, Token Protection, Collision Count Protection) as countermeasures to these attacks.

3. System Model

Sensor network applications range from wild life and environmental monitoring, warehouse inventory, object tracking to military surveillance [22], [23]. In Figure 2, we depict a delay tolerant sensor network with three remote regions. Two of the regions have a large deployment of low-powered sensor nodes. In this scenario, sensor nodes communicate their readings hop-by-hop to fixed sink nodes within their respective domains.

The fixed sinks act as Group Head (GH) to a number of sensors and can perform data aggregation and fusion to reduce duplication. Fixed sinks are more powerful computationally and storage-wise than ordinary sensors. Mobile sinks (human, vehicular, any mobile object with a PDA-type device) can be used to collect data from fixed sinks in a scheduled manner to reduce forwarding cost, balance communication load and extend the life of the network.

The mobile sinks use wireless communication when in range to collect sensor data. Packets must be authenticated before storage or forwarding. The hierarchical organization is to conserve energy and network bandwidth. We assume that an Offline Security Manager (OSM) exist during the initialization of the system to handle the key generation and distribution of secret credentials. Key revocation is out of scope of this work.

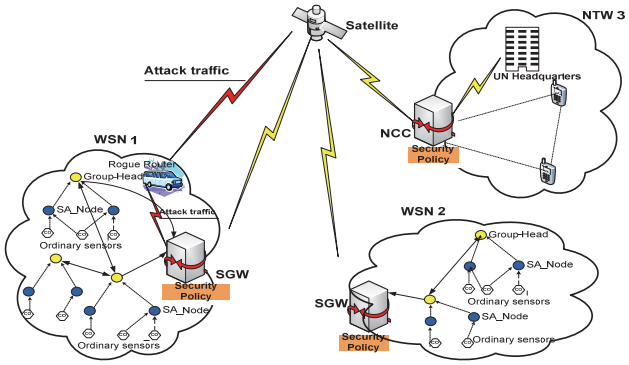

Figure 2. A DTN Showing Three Disjoint Regions

A. Attacker Model

We assume that the attacker can inject bogus packets into the network by flooding. The aim is to keep DTN nodes busy, drain limited resources and introduce network latency. We assume that the computational power of the attacker is large and he can compute crypto-functions and Message Authentication Codes (MACs) with great efficiency and speed. The attacker can modify packets but does not have knowledge of network secrets such as keys and nonce values. The attacker is mobile but cannot compromise legitimate nodes.

B. Mobility Model

We use a combination of Map-based and Random Way Point (RWP) movement models [10] for our simulations. Fixed sinks and sensor nodes are modelled to be stationary and use Bluetooth interface to communicate. Mobile sinks are modelled as cars having speeds ranging from 7-10km/h. Attackers use the RWP movement model uniformly distributed moving at random speeds of 2-10km/h. Attackers use Bluetooth or High-speed interfaces to communicate.

C. Routing Model

In our simulations we use Spray and Wait routing which is a replication-based routing protocol to model the

routing scenario. Other DTN routing protocols that can be used include MaxProp, Epidemic and Prophet [10].

C. Design Goals

All relayed packets must be authenticated in order to filter and drop bogus traffic injected by the attacker. The DOS resilience mechanism should be light-weight and not be a target of new attacks. The DOS mechanism should not add overheads in term of additional packets to the network. The mechanism should be able to secure the DTN and improve the performance of the network and the security service (low communication and computational overheads respectively). We are also particular about storage overheads since nodes are constrained in terms of memory.

D. Networking and Security Requirements

It is important that a DOS filter mechanism should be able to withstand significant node mobility, run efficiently on resource-limited nodes like sensors and be resilient to delays in the order of minutes, hours or days. The mechanism should support varying data rates and withstand changes in contact times. In the absence of an end-to-end path, the mechanism should be able to operate efficiently.

In terms of security requirements we use nonce and timestamps to ensure freshness, drop expired bundles and thwart replay attacks. We check every bundle for integrity to prevent data content modification. Every bundle must be authenticated to ensure that they originate from legitimate sources.

E. Assumptions

We assume that a large number of nodes in the DTN are resource-constrained. Malicious nodes are mobile, gateways are stationary. We assume that security policies and cryptographic credentials have been distributed prior to any form of communication.

4. The Proposed Security Scheme

4.1 Intra-Regional DOS Mitigation

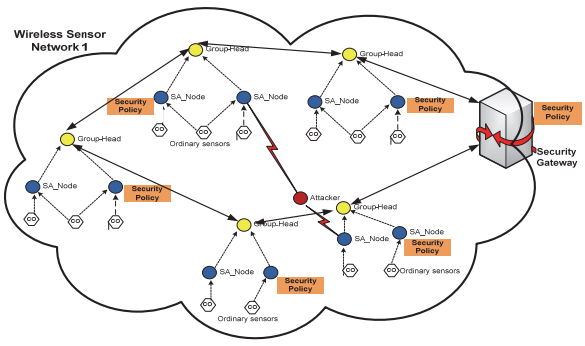

Figure 3. Intra-Regional DOS Scenario

A robust and effective DOS resilience mechanism should have a Detection, Classification and Response element [8]. A generic DTN bundle is made up of the primary block and the payload block. Figure 4 shows that additional blocks like the Bundle Authentication Block (BAB), Payload Integrity Block (PIB), and Payload Confidentiality Block (PCB) can be added to a bundle to provide security [19].

To provide DOS-resilience in DTN, we propose a new security extension block called a DTN-Cookie block. This block provides light-weight message authentication and reduces the computational overhead associated with resource intensive signature verification.

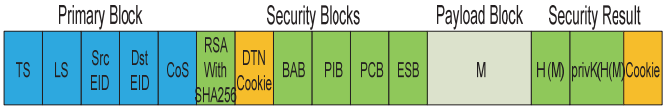

Figure 4. A DTN Bundle with Security Extension Blocks

TS: the timestamp is a concatenation of a bundle creation time and a monotonically increasing sequence number. TS is unique for every new bundle from a Source Endpoint Identifier (EID)
LS: the bundle lifespan or expiration time. The LS value of a bundle can be in minutes, hours or days
Src_EID: the Source EID of a bundle, each EID is assumed to be a singleton
Dst_EID: the Destination EID i.e. the entity for which the bundle is destined.
CoS: The sender's class-of-service rights. A bundle can have an expedited, normal or bulk CoS.
RSAwithSHA256: represents the cipher suite
PIB: the Payload Integrity Block, assures the authenticity and integrity of the bundle
PCB: the Payload Confidentiality Block, indicates that some parts of the bundle has been encrypted at the source
ESB: Extension Security Block
M: the bundle payload
H (M): h is the hash value derived by passing the payload M through the function H. H is a cryptographic hash function such as MD5, SHA1 or SHA256. We will be using SHA256 as the underlying hash function to the signature and MAC algorithms
pubKXi: the public key of node Xi
privKXi: the private key of node Xi.

The Bundle Security Protocol specification [19] provides minimal protection against DOS attacks. DTN nodes simply drop bundles that fail the authentication and access control checks. We have identified resource exhaustion as a simple means of launching DOS attacks and causing availability problems in DTN. For the intra-regional DOS scenario, we propose three variants of DTN-cookie which can be dynamically chosen based on the perceived Network Threat Level (NTL).

$$\text{DTN-cookie} = H((\text{Timestamp} \mid \text{Src\_EID}_x) \mid \text{p-RNG (IV)}) \ldots\ldots\ldots\ldots (v1)$$

The Initialization Vector (IV) is known only to registered nodes of the region. The IV value is used to seed the pseudo-Random Number Generator (p-RNG); the result is a random long integer value. A concatenation of the timestamp and bundle source EID provides a unique bundle identifier. This unique bundle identifier is concatenated with the random long integer and hashed with **H** (the SHA-256 algorithm) to produce a fixed-length hash **h** which is appended to a bundle as DTN-cookie. The IV is changed periodically by the regional security gateway to ensure freshness.

$$\text{DTN-cookie} = H((\text{Timestamp} \mid \text{Src\_EID}_x) \text{ Xor p-RNG (IV)}) \ldots\ldots\ldots \text{ v2}$$

The second DTN-cookie variant (v2) is the result when we perform a bit-wise Exclusive-OR operation on Timestamp|Src_EID_x and p-RNG (IV). | is the concatenation operator, p-RNG (IV) is the same as in v1. This DTN-cookie variant has more randomness and provides a stronger DOS solution.

$$\text{DTN-cookie} = \text{HMAC}((\text{Timestamp}|\text{Src\_EID}_x) \text{ Xor p-PNG (IV)}, K_{RS}) \ldots\ldots\text{v3}$$

The third DTN-cookie variant (v3) is derived in the same way as v2 with SHA-256 as the underlying hash function. The only difference is that the result of the operation is hashed with a regional secret key K_{RS} to produce a fixed-length MAC which we append to every bundle. The mode of generation of the secret key, the use of p-RNG and bit-wise Exclusive-OR operation inputs more randomness to the DTN-cookie. The secrecy of the IV and the key makes the DTN-cookie hard to forge. These values are changed periodically by the security gateway to prevent compromise and ensure freshness.

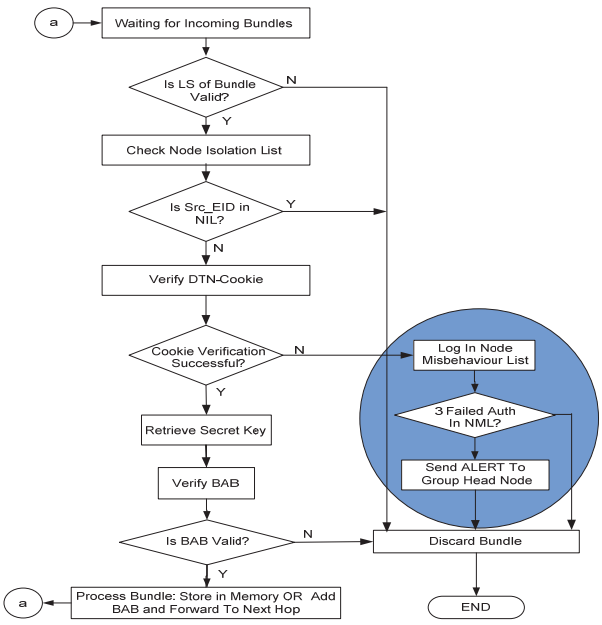

Figure 5. Intra-Regional DOS Mitigation Flow Diagram

When a bundle arrives at a security-aware node, the Bundle Protocol Agent (BPA) examines the bundle to determine if it is a Data or Alert bundle originating from a legitimate source and not expired. Next the BPA tries to determine the perceived Network Threat Level (NTL) associated with the bundle. It does this by looking at the DTN-COOKIE Block. The DTN-COOKIE Block contains the NTL indicator (where Low = 1, Mild = 2, Severe = 3). Based on the NTL indicator, the BPA is able to choose which cipher suite to use to verify the DTN-cookie.

The DTN-COOKIE Block has a trailer block with the security result of the DTN-cookie computation as payload. The BPA can also use the Class of Service parameter to deduce the type of bundle it is dealing with by looking into the CoS field in the bundle primary block. Regions are divided into security domains and Network Threat Levels (NTL) is set by GH nodes in each domain making threat response very localised. Every security-aware node in the DTN maintains a Node Misbehaviour List (NML) and an Alert List (AL). The NML is for recording failed authentication attempts while the AL contains information on blacklisted nodes. These lists are flushed periodically to free memory space. We set a threshold α for failed authentication attempts.

A region is divided into X number of security domains during deployment with one or more fixed sinks per domain to act as Group Head (GH). A GH node can communicate with mobile sinks, other fixed sinks (GHs) and sensors within its transmission range. To reduce communication cost, a sensor node within a security domain sends its sensed data to a GH within its transmission range.

During the authentication process, if a legitimate node records failed authentication attempts above α threshold, it blocks the affected node and sends an alert to notify the GH. Conversely, if a GH records alerts against that same node in excess of a set threshold ß it notifies all sensor nodes within that domain. Packets originating from the blocked address are dropped without any processing.

Table 1. NTL and Corresponding Cookie Variants

Table 1 associates each DTN-cookie variant to a NTL value. This helps security-aware nodes to determine which cookie variant to apply at any point in time. This design makes the solution adaptive to varying threat intensities and saves battery power. Egress filtering is used to stop attackers spoofing their addresses to mount an attack. Also we limit the rate at which a node can send packets per connection at any given timeframe to prevent flooding using bogus packets.

Network Threat Level (NTL)	NTL Classification	Cookie Type
NTL1	LOW	Variant1 (v1)
NTL2	MILD	Variant2 (v2)
NTL3	SEVERE	Variant3 (v3)

4.2 Inter-Regional DOS Mitigation

It is important to secure the inter-regional segment of DTN communications to ensure availability of services. Disjoint regions can be connected either by a bus, ship, satellite that act as a data mule or relay. In this communication scenario we assume that gateways are powerful workstations with large storage and processing capabilities. To prevent the attacker from spoofing addresses, ingress filtering is enforced at the gateways. Communication between regions is gateway-to-gateway. The composition of DTN-cookie used for gateway-to-gateway communication is given:

DTN-cookie=HMAC ((Timestamp|Src_EID$_x$) Xor p-PNG (IV), K_S)…v3

The DTN-cookie is same as the v3 used in intra-regional communication. The subtle difference is the use of an inter-regional symmetric key K_S. Figure 2 gives a clear picture of a DTN where it is possible for disjoint and often remote regions to communicate. In the depicted scenario, the satellite acts as a relay node to provide connectivity.

In our proposal we use the v3 DTN-Cookie to provide DOS resilience in this scenario. The security gateways are workstations with enormous storage, CPU processing and power capabilities. The gateways enforce ingress filtering and bundles are processed if they have genuine source addresses. Attacks launched through address spoofing are detected during the cookie verification stage. The attacker does not possess the network secrets required to generate an authentic bundle. The processes shown in Fig. 4 also apply in this scenario.

Variable nonce values are used to seed the pseudo-random number generator in different time-slots. The security gateways are required to be loosely time-synchronized. Communication time is divided into equal timeslots for (say) 2 hours with each time slot having its associated nonce value. For example [0-2]: N_1, [2-4]: N_2, [4-6]: N_3, [6-8]: N_4, [8-10]: N_5… [22-24]:N_{12}. [0-2]… [22-24] represent the timeslots and $N_{1...}$ N_{12} are the respective nonce values.

The ingress filtering policy requires all in-bound bundles to have a BAB, PIB and PCB block. The BAB should be used for integrity and sender-side authentication. The BAB to be a digital signature using asymmetric cipher suite (RSA-SHA256). To save power, we restrict communication in this scenario to be gateway-to-gateway given the limited power budget of wireless mobile nodes. This is to enhance the survivability of the network and prevent mobile rogue routers from keeping the satellite busy with fake or mal-formed bundles during each pass of the satellite. Payload encryption is required in gateway-to-gateway communications for both maintenance traffic and data bundles. Also rate limiting techniques can be used to police the network interfaces at the security gateways to guard against flooding attacks.

A. Synchronizing the Gateways

Time-synchronization is an important aspect to be considered when designing a mechanism to provide DOS-resilience in DTN. In [24], the authors elaborate on the use of timestamps and the need for time synchronization. Initial pre-shared symmetric keys between Sensor Gateway at the headquarters (SGW_{HQ}), Sensor Gateway 1 (SGW_{WSN1}) and Sensor Gateway 2 (SGW_{WSN2}) are assumed. The security gateways have a common view of time (say UTC) irrespective of their time zones. Also, the p-RNG functions at the security gateways have a uniform initial seed value (N_o). Communications among the gateways is initiated by the SGW_{HQ} by sending two different N_1 nonce values to SGW_{WSN1} and $SGW_{WSN2.}$ The nonce is the bundle payload and is encrypted using the public key of SGW_{WSN1} and SGW_{WSN2}. The SGW_{HQ} signs the bundles using its private key, calculates the DTN-cookie, appends it to the bundles and sends to the gateways.

At the gateways, the timestamp, CoS and sender EID are retrieved from the bundle and based on the pre-shared symmetric keys (K_S) between the SGW_{HQ}, SGW_{WSN1} and SGW_{WSN2}. The DTN-cookie is computed and compared to that on the received bundle. The bundle is silently dropped if the DTN-cookie verification is unsuccessful. On the other hand, if the verification is successful we proceed to test the integrity of the BAB (digital signature). Each SGW_{WSN} uses the public key of the SGW_{HQ} to verify the signature. If the signature verification fails the bundle is dropped because its content is considered modified on transit. If the verification of signature is successful, we proceed to decrypt the payload. Each SGW_{WSN} uses its private key to decrypt the payload which is the new reference nonce for communications. Attackers within the satellite's coverage are able to see every communication since the satellite uses a broadcast channel. To prevent eavesdropping of the nonce value, we encrypt the payload. We define a bound for the generation of nonce values as follows: $0 < N_i < 999999$ where i is a positive integer. If the N_i value generated is greater than the defined upper-bound, the entire seed generation process is started all over again.

A security gateway with data to send first chooses a random number within the pre-defined bound which it uses as seed to the p-Rng function. The result of this operation is a nonce which it sends to a destination gateway. This is done following the steps described earlier above. The gateways remain synchronized using previous nonce values as seed to the p-Rng function. Where initial nonce equals N_o, N_1 = p-Rng (N_o), N_2 = p-Rng (N_1), N_3 = p-Rng (N_2) forming a hash-chain of nonce values.

DTN-cookie=HMAC ((Timestamp|$EID_{HQ\text{-}SGW}$) Xor p-RNG (S_i), K_S)

One important property of one-way hash chains is that intermediate values can be recomputed using subsequent values in the chain. Bundles that arrive after their timeslot

can still be processed if they are not expired. Also SGW_{WSN1} and SGW_{WSN2} can communicate with each other via the satellite and can remain synchronized by following the steps as described.

5. Simulation Results and Performance Evaluation

We present the results obtained using the ONE simulator which show the performance of the proposed DOS mitigation mechanism. We run the simulation with 10 mobile nodes deployed and distributed uniformly in a 4500 by 3400 meters area. The average speed of each node varies between 7-10km/h and the transmission range of each node is 100m. Legitimate nodes generate 1 packet every 60-120 seconds. The attacker generates 1 packet per second. Each attacker node generates 60 packets per minute. A summary of the simulation parameters is shown in table 2.

Table 2. Simulation Configuration

Simulation Time	12 Hours
Bandwidth	250kBps
Transmission Range	100m
Buffer size	5M
Number of Nodes	10
Message size	64kB
Message Generation Interval	60-120s
Message Time-to-live	300s
Routing Protocol	Spray and Wait
Number of forwarding copies	2
Mobility Scenario	Helsinki City Model

Our analysis is based on three metrics: packet delivery ratio, average latency and energy efficiency. Delivery ratio is the proportion of messages generated to the number of messages successfully delivered. Average latency measures the average delay experienced by a delivered packet. Energy efficiency measures the energy consumption of nodes

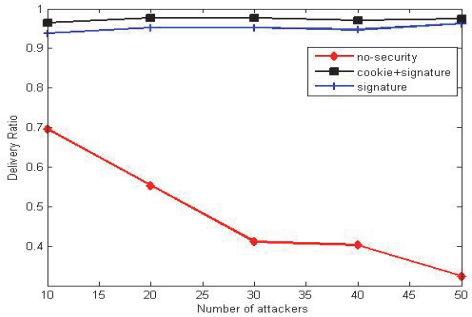

Figure 6. Packet Delivery Ratio with Increasing Number of Attackers

In Figure 6, we show the effects of attackers on the packet delivery ratio. When no security mechanism is adopted the delivery ratio declines steeply with an increase in number of attackers in the network. The delivery ratio shows a remarkable improvement when we apply security mechanisms to counter the attack. Our DOS resilience mechanism (cookie+signature) shows a 2.2% improvement over RSA-1024 signature verification algorithm (signature).

In Figure 7, we analyse the effects of an increasing number of attackers on the average latency. Latency in a communication system is affected by the propagation, transmission, processing and queuing delays especially in multi-hop routing. With no security mechanism adopted even with an increase in number of attackers the average latency drops. The reason is two fold: the attacker does not accept or buffer packets from other nodes. Secondly, no security processing is performed by the nodes.

There is a slight increase in latency when we activate our DOS mechanism (cookie+signature). This is as result of processing of the DTN-cookie which is negligible. The amount of latency increases dramatically when RSA-1024 signatures is used as the protection mechanism. The high processing load introduces congestion which leads to very high latency levels. The results show that the proposed DOS resilience mechanism is robust and scales as the number of attackers increase.

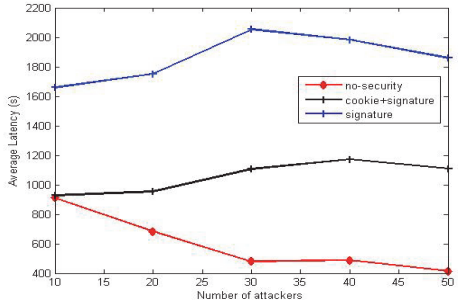

Figure 7. Average Latency with Increasing Number of Attackers

One of the main objectives of this paper is to optimize computational and communication costs by providing security in DTN in an energy-efficient manner. Our proposed mechanisms use hash functions, HMAC and symmetric key cryptography which impose less energy cost on the nodes during authentication.

Our evaluation is based on the work in [22] which shows that a SHA1 operation requires 0.76µJ/B. A HMAC operation requires 1.16µJ/B of power while RSA-1024 requires 270.13mJ for key generation, 546.5mJ for *Sign* operation and 15.97mJ for *Verify*. From this analysis it is evident that the computational cost of the proposed DTN-cookie mechanism is negligible when compared to digital signatures.

In terms of communication cost, our mechanisms do not add any additional packets into the network. The only overhead is the per-packet additions in terms of DTN-cookies. This is largely dependent on the routing/ forwarding replication strategy.

Data transmission cost (transmit and receive) is greater than the computation cost. An experiment conducted by

[25] on the Mica2dot platform show that the cost to receive and transmit one byte of data is 28.6μJ and 59.2 μJ respectively. When our mitigation mechanism is activated, packets from the attacker are identified quickly and dropped at the first hop. This helps to save transmission energy and bandwidth. Every one byte per hop of an attacker's data that our scheme drops translates to (28.6μJ + 59.2 μJ) = 87.8 μJ of energy savings.

Next we evaluate the strength and resilience of our mechanisms against attacks. Each packet has a timestamp embedded in it. The concatenation of the timestamp and source_EID is a unique packet identifier which provides a strong feature for thwarting replay attacks. Any attempt to modify the timestamp is detected during DTN-cookie verification. The payload is protected using a digital signature. The BSP specification recommends RSA-1024 as the de facto digital signature algorithm for DTN but recent studies shows that Elliptic Curve Cryptography (ECC) is suitable for sensor networks. The Elliptic Curve Digital Signature Algorithm ECDSA-160 supports 160-bit keys and provides the same level of security as RSA-1024 [25]. ECDSA-160 has a smaller key and signature size which makes it more energy efficient than RSA-1024 [26], [27].

The use a cryptographically secure random number generator and secret nonce values make the proposed mechanisms random and hard to forge**.** The v1 and v2 DTN-cookie variants use SHA-256 as hash function. SHA-256 is a 256-bit hash function which uses 32-bit words and provides 128 bits of security against collision attacks [28]. The hash operation produces a fixed-length DTN-cookie which saves memory, CPU processing and provides integrity to packet fields.

As a requirement, H can be applied to a block of data of any size, and it is relatively easy to compute H(x) for any x. For any given value h it is computationally infeasible to find $y \neq x$ such that H(y) = H(x) (weak collision resistance). Finally it is computationally infeasible to find any pair (x, y) such that H(x) = H(y) (strong collision resistance) [28]. The v1 and v2 DTN-cookie variants have all these properties in-built.

The third DTN-cookie variant uses HMAC, a mechanism for message authentication and uses SHA-256 and a secret key. The cryptographic strength of HMAC is dependent on the properties of the underlying hash function and the bit length of the key. On average an attack will require $2^{(k-1)}$ attempts on a k-bit key.

The amount of effort needed for a brute-force on a MAC algorithm can be expressed as min (2^k, 2^n). The key and MAC lengths should satisfy the relationship min (k, n) ≥ N, where N is in the range of 128 bits [28]. The irreversibility property of the one-way hash function and the secrecy of the symmetric keys (K_S, K_{RS}), makes the proposed DTN-cookie hard to forge.

6. Conclusions

In this paper, we have discussed the problem of DOS attacks in energy constrained DTN environments. We have pointed out that strong and resource demanding security is vulnerable to resource exhaustion attacks. Three DTN-cookie variants have been proposed to address this problem in DTN hop-by-hop authentication.

Our scheme can identify and drop bogus packets from the attacker, block attack packets from being processed and does not introduce a new availability problem when activated. The proposed mechanisms are light weight and hard to forge. Simulation results show the performance of our mechanisms and demonstrate the effectiveness and efficiency of our scheme. As future work, we intend to investigate compromised node detection.

References

[1] Ott, J. and Pitkänen, M.J. (2007) DTN-based Content Storage and Retrieval. *In Proc. Int'l World of Wireless, Mobile and Multimedia Networks*, 1-7, 2007.

[2] Khabbaz M.J. Assi C.M and Fawaz W.F. (2010) Disruption Tolerant Networking: A Comprehensive Survey on Recent Developments and Persisting Challenges. *IEEE Communications Surveys and Tutorials,* Vol. PP, Issue 99, 1-31, May 2011

[3] Musolesi, M. and Mascolo, C. (2008) A Framework for Multi-Region Delay Tolerant Networking. *In Proc. ACM WiNS-DR'08*, 37-42, Sept., 2008

[4] Samuel, H. and Zhuang, W. (2010) Preventing Unauthorized Messages and Achieving End-to-End Security in Delay Tolerant Networks. *Journal of Communications,* Vol. 5, No.2, 152-163, 2010

[5] Raymond, D.R. and Midkiff, S.F. (2008) Denial of Service in Wireless Sensor Networks: Attacks and Defenses. *IEEE Pervasive Computing,* Vol.7, Issue 1, 74-81, 2008

[6] Xing, F. and Wang W. (2006) Understanding Dynamic Denial of Service Attacks in Mobile Ad hoc Networks, *Military Communications Conference*, 1-7, 2006

[7] Mölsä, J. (2006) Mitigating Denial of Service in Computer Networks, *Helsinki University of Technology, Finland,* TKK Dissertations 32, 2006

[8] Loukas, G. and Öke G. (2009) Protection against Denial of Service Attacks: A Survey. *The Computer Journal,* 53, 1020-1037, 2010

[9] Onen, M. and Molva, R. (2004) Denial of Service Prevention in Satellite Networks. *IEEE Int'l Conference on Communications,* Vol. 7, 4387-4391, 2004

[10] Keränen, A. Ott, J. and Kärkkäinen, T. (2009) The ONE Simulator for DTN Protocol Evaluation. *SIMUTools'2009* Rome Italy, 2009

[11] Dwork, C. and Naor, M. (1998) Pricing via Processing or Combating Junk Mails. Springer, Heidelberg, 1998

[12] Juels, A. and Brainard, J. (1999) Client Puzzles: A Cryptographic Countermeasure against Connection Depletion Attacks. *In Proc. Network and Distributed Systems Security Symposium*, 151–165, 1999

[13] Maughan, G. Schertler, M. Schneider, M. Turner, J. (1998) Internet Security Association and Key Management Protocol (ISAKMP), RFC 2408, 1998

[14] Meadows, C. (1999) A Formal Framework and Evaluation Method for Network Denial of Service. *In Proc. IEEE Computer Security Foundations Workshop,* 1999

[15] Wood, A.D. and Stankovic, J.A. (2005) A Taxonomy of Denial-of-Service Attacks in Wireless Sensor Networks, *Handbook on Wireless Sensor Networks, Compact Wireless and Wired Sensing Systems,* Print ISBN: 978-0-8493-1968-6, 2005

[16] Perrig, A. Szewczyk, R. Wen, V. Cullar, D. and Tygar, J.D (2001) Spins: Security Protocols for Sensor Networks. In Proc. Of MobiCom, 189-199, 2001

[17] Wang, R. Du, W. and Ning, P. (2007) Containing Denial-of-Service Attacks in Broadcast Authentication in Sensor Networks, *ACM MobiHoc'07,* 9-14, 2007

[18] Deng, J. Han, R. and Mishra, S. (2005) Defending against Path-based DOS Attacks in Wireless Sensor Networks, *ACM SASN'05*, 2005

[19] Symington, S. Farrell, S. Weiss, H. Lovell, P. (2011) Bundle Security Protocol Specification, Draft-irtf-dtnrg-bundle-security-19, May 2011

[20] Burgess, J. Bissias, G.D. Corner, M. and Levine, B.N. (2007) Surviving Attacks on Disruption-Tolerant Networks without Authentication. *In Proc. ACM MobiHoc'07,* 67-70, 2007

[21] Uddin, M.Y. Khurshid, A. and Dung H.D. (2010) Denials In DTNs. *Technical Report: http://hdl.handle.net/2142/14821*, 2010.

[22] Potlapally, N. Ravi, S. Raghunathan, A. and Jha, N. (2003) Analyzing the Energy Consumption of Security Protocols, *ACM ISLPED'03*, Seoul Korea, 2003.

[23] Oh, Y. Ning, Peng. Liu, Y. and Reiter, M. (2009) Authenticated Data Compression in Delay Tolerant Wireless Sensor Networks, *INSS'09,* 1-8, 2009

[24] Ansa, G. Cruickshank, H. and Sun, Z. (2011) A Proactive DOS Filter Mechanism for Delay Tolerant Networks. *2nd ICST PSATS, Conference*, Malaga Spain, February 2011

[25] Wander, A.S. Gura, N. Eberle, H. Gupta, V. and Shantz, S.C. (2005) Energy Analysis of Public-Key Cryptography for Wireless Sensor Networks. *In Proc. of PerCom'05*, 324-328, March, 2005

[26] Arazi, O. Qi, H. and Rose, D. (2007) A Public Key Cryptographic Method for Denial of Service Mitigation in Wireless Sensor Networks*, IEEE SECON'07,* 51-59, 2007

[27] Ren, K. Yu, Shucheng Lou, W. and Zhang, Y. (2009) Multi-user Broadcast Authentication in Wireless sensor Networks, *IEEE Transactions on Vehicular Technology,* Vol. 58, No. 8, 2009

[28] Krawczyk, H. Bellare, M. and Canetti, R. (1996) HMAC: Keyed-Hashing for Message Authentication, *Crypto 1996*, 1-15, 1996