Access Control Framework for Delay/Disruption Tolerant Networks

Enyenihi Johnson, Godwin Ansa, Haitham Cruickshank, and Zhili Sun

Centre for Communication Systems Research (CCSR)
University of Surrey, Guildford, United Kingdom
{e.johnson,g.ansa,h.cruickshank,z.sun}@Surrey.ac.uk

Abstract. The emergence of DTN as an option for sustaining communication in environments with high delay/frequent disruption have rendered existing access control mechanisms inappropriate hence the need for a new concept in DTN access control. This is primarily due to contradicting assumptions like low delay and constant connectivity on which the existing mechanisms are built. This paper discusses the security issues in DTN, investigate existing access control mechanisms and relate their design principles as well as operational mode to DTN. We proposed a lightweight hierarchical architecture based on AAA architecture concept and explored the DTN architecture to identify those features that will support the implementation of AAA architecture concept. We present the proposed architecture for an intra-domain scenario with a brief description.

Keywords: DTN, Security, Access Control, AAA, Authentication, Authorization, Hierarchical.

1 Introduction

Advancement in technology and the quest for effective communication have led to the discovery of networks that are delay/disruption tolerant where some of the assumptions on which today's Internet was built no longer hold. These networks ranging from marine networks, mobile ad-hoc networks, wireless sensor networks, military tactical networks to deep-space networks all share a common problem. This common problem is their inability to sustain communication in the face of limitations like intermittent connectivity, high/variable delay, asymmetric data rates, high error rates and heterogeneity. To address this problem, the Delay/Disruption Tolerant Networking (DTN) [1], [2] was proposed and the overlay network approach [3] was considered the most appropriate. Its emergence opens new areas of research in security which includes key management, Denial of Service (DoS) attacks, anonymity and privacy, access control amongst others. Access control is the main focus of this paper.

The need to have a common platform to carry out DTN services necessitated the introduction of a new layer called the bundle layer. The inability of the current Internet protocols to address communication problems in delay/disruption tolerant networks led to the development of DTN protocols (Bundle Protocol and Licklider Transmission Protocol) [4]. Our framework is designed to implement the Bundle Protocol [5] baring

K. Sithamparanathan et al. (Eds.): PSATS 2010, LNICST 43, pp. 249–264, 2010.

its complexity [6] because apart from being an overlay protocol, it has an in-built security mechanism to provide end-to-end data integrity and confidentiality as well as protecting the network from unwanted traffic [7]. References [1] - [9] are the existing documentations that give detailed description of DTN, its architecture and security.

The primary goal of this paper is to propose an access control framework for delay/disruption tolerant networks. To realise the goal, we evaluate security issues in DTN and identify access control related threats. We investigate existing access control mechanisms and relate their design principle as well as operational mode to DTN. We examine the DTN architecture and identify those features that support access control implementation. We propose a lightweight hierarchical architecture and justify why it suits the DTN environment.

This paper is organized as follows: In section II we review security issues in DTN, section III discusses access control and existing traditional solutions, section IV discusses the AAA architecture mentioned in [8] and the applicability of its concept in DTN access control, section V describes the DTN architecture and the existing features that supports the implementation of AAA architecture concept, section VI presents and explains the proposed access control framework, and section VII presents the conclusions.

2 DTN Security

The inherent constraints (like long delay, frequent disconnection and heterogeneity) in DTN and the overlay nature of the bundle protocol make security in DTN a critical issue. The inability of existing security mechanisms to address security issues in DTN environment necessitated the need for an entirely new concept in DTN security. This led to the identification of some threats during the design process of DTN security mechanisms. The identified threats according to [9] are those associated with non-DTN node, resource consumption, denial of service, confidentiality and integrity as well as traffic storm. The resource scarcity nature of the DTN demands that resource consumption related threats [9] associated with masquerading and modification attacks [10] is given serious consideration. Masquerading attack is where a malicious attacker impersonates another legitimate entity to gain access to secret information in a system or network in the case of an outsider, or to enjoy more privileges in the case of an insider. Modification attack is where an attacker attempts to modify information it is not authorized to. It exists in the form of changing existing information, removal of existing information and insertion of information.

DTN security is described extensively in [9], [11] and its goal is to ensure the protection of DTN infrastructure from these attacks through:

- Denying access to unauthenticated entities
- Preventing unauthorized entities from controlling the DTN infrastructure
- Preventing authenticated entities from carrying out unauthorized services
- Prompt detection and discarding of bundles sent by unauthorized entities
- Prompt detection and discarding of bundles with modified headers
- Prompt detection and removal of compromised entities

The above listed DTN security goals can be realised with access control [11].

3 Access Control

Access Control protects the network from unauthenticated entities and prevents unauthorized entities from using network resources. Reference [12] list and explain the three access control system abstractions of policy, mechanism and model. Access control can be implemented using either a centralized architecture [13] or a decentralized architecture. The decentralized architecture is either distributed [14], [15] where access control decision is fully decentralized or hierarchical [16] where access control decision is partially decentralized. A single entity manages access control in a centralized architecture while the regional security gateways are responsible for access control management in the distributed architecture. In the hierarchical architecture with combined elements of centralization and decentralization, a central entity manages access control of the network comprising the various distinct regional security gateways. The absence of an existing access control solution for delay/disruption tolerant networks to the best of our knowledge necessitated the investigation of traditional access control solutions to ascertain their suitability for the DTN environment.

Reference [12] identifies Discretional Access Control (DAC), Mandatory Access Control (MAC) and Role-Based Access Control (RBAC) as the three main traditional access control policies (solutions). Their brief descriptions are given below:

- **Discretional Access Control (DAC):** This approach is identity based and leaves a certain amount of access control to the discretion of an authorised user. The heterogeneous nature of the DTN environment makes this approach inapplicable. The absence of real assurance on the flow of information in a system and its vulnerability to Trojan horse attack will encourage modification and masquerading attacks respectively which our proposed framework is designed to address.
- **Mandatory Access Control (MAC):** This approach is rule-based and leaves access control management as well as definition of policy that cannot be modified by an authorized user to the system administrator. The use of system-wide policy and its ability to minimize abuse of applications by granting needed rights to individual participants make the approach suitable for the DTN environment. How this policy is implemented in the DTN environment will determine how limitations like complex configuration and determination of access authorization for each application are handled.
- **Role-Based Access Control (RBAC):** This approach is rule-based and access control decisions are based on roles individual users have as part of an organization. The administrative complexity of this approach increases with increase in granularity since multiple roles per user is needed for stronger security. Fewer roles per user make administration easier while weakening the security. RBAC will not be suitable for DTN environment from the stronger security perspective while it may be suitable from the easier administration perspective. Its combination with MAC is a probable solution.

The conceptualization of DTN to provide interoperability across heterogeneous networks and the need for the implementation of system-wide policy make trust a significant factor in DTN access control. Trust-based access control has been implemented using the centralized architecture with AAA (Authentication, Authorization and

accounting) architecture [17] as an example. The conception of trust management for decentralized access control first mentioned in [20] led to the development of trust management systems that are either based on credential/policy or reputation [21]. The reputation-based trust management system is ideal for homogeneous networks while the credential/policy-based trust management system is ideal for heterogeneous networks. Few existing distributed trust management models used in traditional internet environments are: PolicyMaker [20], KeyNote [22], REFEREE [23] and SPKI [24].

The classical AAA architecture and the above mentioned credential/policy-based distributed trust models are not suitable for direct implementation in DTN due to: design principle, operational complexity, scalability issue and unavailability during long/variable delay and frequent disruption [25], [26]. However, the implementation flexibility offered by the AAA standard and the applicability of certain concepts with slight modification to the DTN environment underlines the suitability of AAA architecture concept to DTN.

4 AAA Architecture

The Authentication, Authorization and Accounting (AAA) architecture shown in fig. 1 is a framework that defines a central entity called the AAA Server to support the AAA operations. The AAA operations are Authentication, Authorization and Accounting but accounting is out of the scope of this work. The three network requirements needed for access control decision making are: the AAA server which receives and processes end users requests; AAA Client/NAS which provides end users with access to the network; and the AAA protocol which conveys AAA information between the NAS and the AAA server. Examples of AAA protocol are RADIUS (Remote Access Dial-In User Service) and DIAMETER. Additional requirements needed by the AAA server to facilitate access control decision making and resource management are:

AAA	Authentication, Authorization and Accounting
NAS	Network Access Server
ASM	Application Specific Module
P&E R	Policy & Event Repository
ASD	Application Specific Database

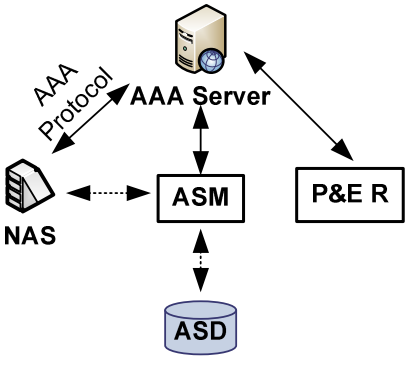

Fig. 1. Generic AAA Architecture

- Application Specific Module (ASM) which houses user database with application specific information.
- Policy & Event repository which stores on-going events as well as information relating to available services, resources and policy rules.

This architecture has a single point of failure, interactive, scalability problem in large networks, uses centralized Access Control List (ACL) amongst others. [17] – [19].

4.1 Authentication

Authentication ensures that the identity of a user requesting access to a system or services is verified before such request is granted. The three types of authentication [19] are:

- ***Client Authentication*** which comes in the form of either user or device authentication uses the credentials presented by the client to verify the authenticity of the client before granting access to the network.
- ***Message Authentication*** whose primary goal is to prevent modification attack ensures the legitimacy of the message source and data integrity while in transit.
- ***Mutual Authentication*** which protects a communicating party during node compromise ensures that two communicating entities at any point in time use either sequential or parallel method to authenticate each other.

Client and mutual authentication are implemented with either two-party model or three-party model [19]. Two-party model facilitates communication between two entities through a direct line without an intermediary node like a gateway or proxy. Three-party model which is our adopted model was designed to address the ineffectiveness of the two-party model in large networks. It engages the services of a third party to ensure that communicating parties only have access to resources and services they are authorized to. These models employ various authentication mechanisms that are classified using the three fundamental criteria of possession, knowledge and identity. Among the few mechanisms listed in [19], Public Key Infrastructure (PKI) scheme is considered for this work because of its numerous advantages.

4.2 Authorization

Authorization decides whether a certain privilege should be given to a user requesting access to the network based on submitted credentials. Entities involved in an authorization process within a single domain are User, AAA Server, and NAS. The User is an entity sending a request; AAA Server is an entity that evaluates the request and makes decision while the NAS is the entity that enforces the decision made by the AAA Server. These entities enter into relationship prior to the authorization phase which is either ***contractual*** (a formal contract or Service Level Agreements between user and the network) or ***trust*** (agreement usually initiated in the form of security association and facilitated by third party authentication server) [18], [19].

The authorization process involves the three messaging sequences of agent, pull and push [18]. The AAA Server is directly involved in entities communication in both agent and pull sequences, and not in a push sequence. Push messaging sequence as illustrated in figure 2 is discussed further because of its peculiarity to the delay/disruption tolerant environment.

Msg 1 is the request to the AAA Server for credential (ticket or certificate), Msg 2 is the response from the AAA Server including the credential and pre-information, Msg 3 is a request for a particular service or forwarding a packet and Msg 4 is a response to the request or acknowledgement of the packet which can be made optional in DTN context. NAS A functions as the User which uses a credential obtained from AAA Server to send a request while NAS B functions as the policy enforcement entity which uses a pre-information from AAA Server to authenticate a requesting party (User). Fig. 2 presents a scenario where communication between NAS A and NAS B does not involve the AAA server directly.

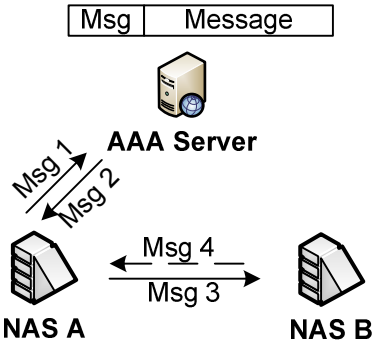

Fig. 2. Authorization Push Messaging Sequence

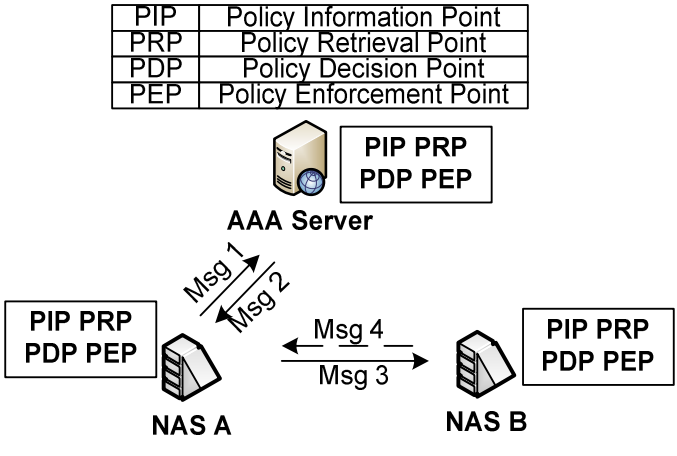

Fig. 3. Modified AAA Policy Distribution Framework

The push messaging sequence as employed in the generic AAA architecture cannot be directly implemented in delay/disruption tolerant networks despite reducing communication exchanges. Modifying the policy distribution framework in [18] to reflect that in fig. 3 will make the push messaging sequence suitable for environment with high delay and frequent disruption. This will make every entity custodian of the four policy elements of PIP and PRP for policy retrieval, PDP for policy evaluation and PEP for policy enforcement.

Worthy of note is the complexity and overhead that will result from this modification. The fragile nature of DTN demands a simple solution and the proposed lightweight hierarchical framework is not designed to provide complex solution. While this concept will be adopted for our proposed framework, we will avoid the use of policy elements and rather programmed the designated components to provide functionalities associated with the various policy elements.

5 DTN Architecture and AAA Concept Implementation

This section examines the DTN architecture [2] and its suitability to implement the AAA architecture concept. The DTN bundle node is the main component of the DTN architecture implementing the bundle layer. The bundle node comes in three different variants of host, router and gateway with persistent storage and custody transfer capability [5]. The host while acting as the source or destination sends or receives bundles but does not forward; the router forwards bundles within a single DTN region; while the gateway forwards bundles between two or more DTN regions and also provides conversions between the lower-layer protocols of the regions involved in bundle

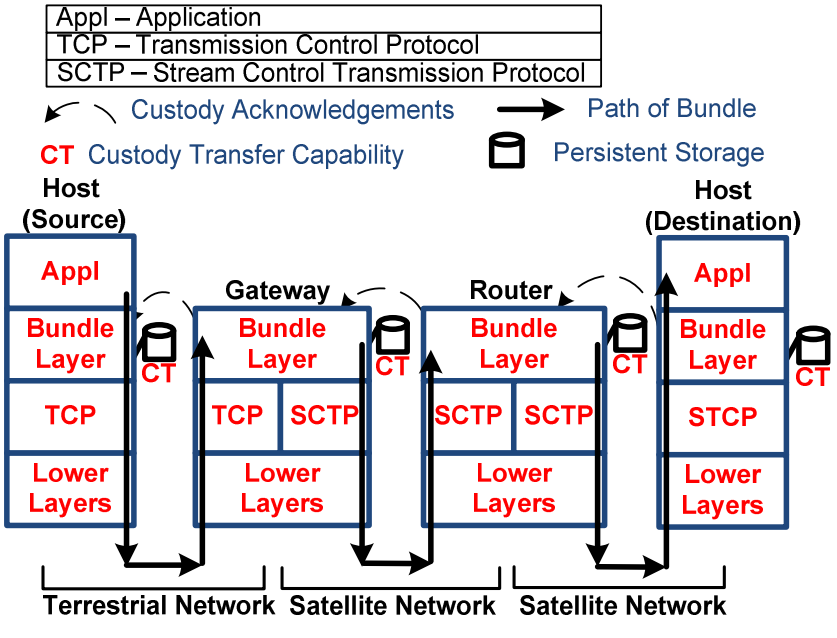

Fig. 4. Basic DTN Architecture

transmission. Fig. 4 shows the basic DTN architecture with the bundle node variants involved in bundle transmission between terrestrial and satellite networks.

The DTN bundle node with its components described in detail in [5] is represented in fig. 5. The three components of the DTN bundle node are:

- Bundle Protocol Agent (BPA)
- Convergence Layer Adapters (CLAs)
- Application Agent (AA) subdivided into Application Specific Element (ASE) and Administrative Element (AE).

The BPA executes the bundle protocol procedures and offer Bundle Protocol (BP) services, CLAs send and receive bundles on behalf of the BPA utilizing services of the lower layers, while the AA through ASE and AE effects purpose-specific communication through BP services utilization [5]. Comparison of the DTN bundle node structure of fig. 5 with the generic AAA architecture of fig. 1 reveals some similarity between them. The BPA, ASE and AE of the bundle node either have similar functions to the AAA Server, Application Specific Module (ASM) and Policy & Event Repository (P&E R) of the AAA architecture respectively or have the capacity to provide similar functions.

Using BP SInt between BPA and ASE, and Prv CInt between BPA and AE makes communication between the BPA and the AA components independent. This is similar to the generic AAA architecture where communication between AAA Server and ASM is independent of that between AAA Server and P&E R. The existence of a common interface (BP Sint) between BPA and ASE as well as AE depicts the possibility of unifying the functions of ASE and AE which might be an advantage. With reference to section 4.2, BPA is designed to execute functions associated with PRP, PDP and PEP while ASE and AE are designed to execute functions associated with PIP.

BP	Bundle Protocol	CLA	Convergence Layer Adapters
BP SInt	BP Service Interface	ASE	Application Specific Element
Pr CInt	Private Control Interface	AE	Administrative Element
BPA	Bundle Protocol Agent	AA	Application Agent

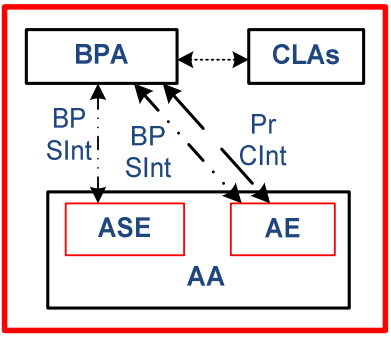

Fig. 5. Abstracted DTN Bundle Node Structure

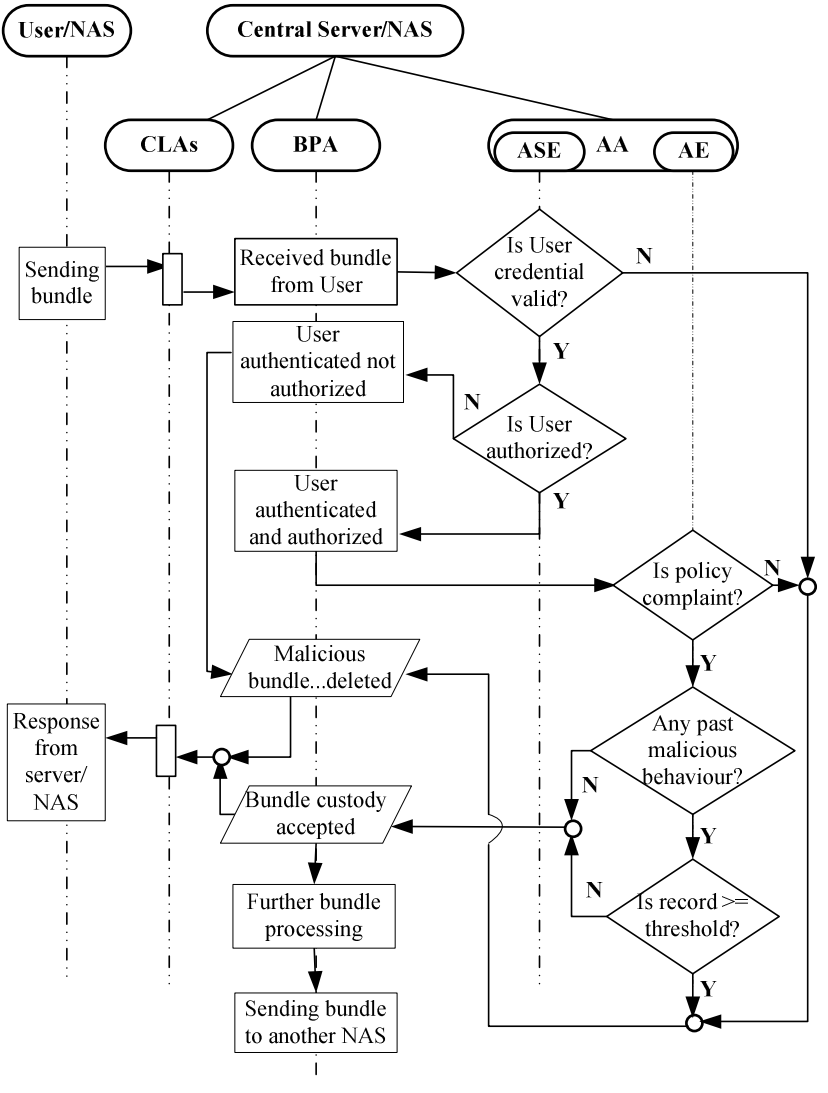

Fig. 6. Proposed Access Control Sequence in DTN Bundle Node

The ability of the bundle node to incorporate BPA, ASE and AE in its internal structure compared to the AAA architecture where AAA Server, ASM and P&E R are external makes it suitable for offline processing and internal decision making. The bundle node with its persistent storage can conveniently store the credential and pre-information used in access control decision making in the generic AAA architecture. Its ability to serve as policy enforcement point where it has and enforce its own policy is emphasized in [7]. The bundle node can be implemented as a server or a gateway (access server) [5], [8] and implements the Bundle Protocol (BP) [5] which is designed to fulfil the minimum requirement of the AAA protocol defined in [18].

Fig. 6 is a flowchart showing the proposed authentication and authorization sequence when the bundle node of fig. 5 is implemented either as a central server or network access server.

The flowchart in fig. 6 incorporates the three DTN bundle node components of CLA, BPA and AA with more emphasis on BPA and the AA sub-components of ASE and AE. Emphasis is placed on what happens when a node receives a bundle because access control is better enforced with the node in the receiving mode. The ASE stores the credentials like keys and certificate from the central server (CA) while AE stores the policy and history of past activities like malicious behaviour of a particular entity. The number of times the malicious activity of a particular entity must not equal or exceed is called the threshold. When the BPA receives a bundle through the CLA, it sends the requesting User's credential to ASE for verification. BPA evaluates the response from ASE to decide whether the User is authenticated and authorized. If the User is authenticated and authorized, the BPA then confirms the User's reputation and conformity with existing policy through the AE. The BPA then evaluates the response from AE to decide whether the bundle should be accepted for custody or not. Whatever action BPA enforces is communicated to the requested user through the CLA. If the bundle custody is accepted, the BPA then proceeds with further bundle processing.

6 The Proposed Architecture

The inability of the existing access control mechanisms to address access control issues in delay/disruption tolerant networks led to the identification of the following desirable features of a workable DTN access control mechanism:

- Separating authentication from authorization
- Supporting offline processing and internal decision making
- Reducing communication exchanges and overheads
- Simplicity and scalability

Based on these features, lightweight hierarchical access control architecture shown in fig. 7 is proposed based on the AAA architecture concept.

The preference for hierarchical architecture is because of the need for a central entity to manage the activities of the various autonomous PNs and the AAA architecture concept because:

- The AAA standard offers implementation flexibility
- The components of the generic AAA architecture provide similar functionalities to that of the DTN bundle node
- The three-party authentication model establishes trust and facilitates communication in heterogeneous environment
- Authorization push messaging sequence reduces communication exchanges and puts less load on the server
- The policy distribution framework can be modified to suit the DTN context

The architecture of fig. 7 assumes a single domain with three private networks and is designed to operate in a conflict scenario like United Nation Peace Keeping Mission. These private networks represent Peace Keeping Forces of three different nations

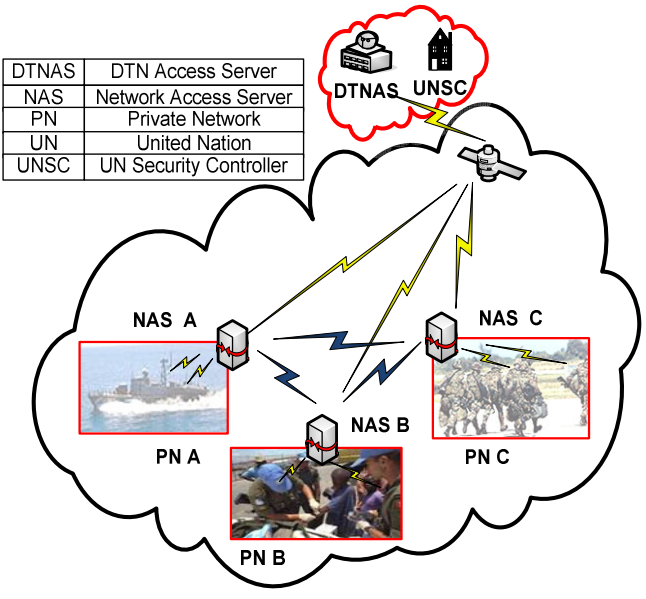

Fig. 7. Proposed Hierarchical Lightweight Access Control Framework

deployed to different locations within a conflict region. The private networks are sensor-based with few DTN-aware nodes. The DTN network comprises the DTNAS, NAS of the private networks and the few DTN-aware nodes within the PNs with satellite facilitating communication in the network. The security gateways (NASs) of the various PNs functions as both bundle and security sources and destinations with security zone [7] existing between them. Each NAS can add and process security blocks. The reference security blocks according to [7] are Bundle Authentication Block (BAB), Payload Integrity Block (PIP), Payload Confidentiality Block (PCB) and Extension Security Block (ESB).

6.1 Architecture Components and Functions

The major components of the architecture of fig. 7 are the UNSC, DTNAS and NAS. These components are described below:

- UNSC: This is the entity that registers all the private networks (countries) designated for Peace Keeping Mission and the organization commissioned to provide the DTN services. The security information obtained during this period is stored and made available to the relevant entities at different times prior to network registration/service initialization phase.
- DTNAS: This is the central server that coordinates the activities of the DTN network and registers the various Network Access Servers (NAS) into the DTN Network. During network registration and service initialization phase, the DTNAS generates and distributes Common Communication Parameter (CCP) and Certificates to all authenticated members accompanied with its public key. The CCP is used by network members

for proof of authentication while the Certificate is used to verify the validity of users' request. The DTNAS can function as Key Server/Key Distribution Centre (KDC) or Certificate Authority (CA).

- NAS: These are security gateways that handle regional access control management. These servers authenticate and register entities into the respective private networks and have the capacity to generate CCP and Certificates needed within the Private Networks (PN) for communication and verification of the validity of users' request. These security gateways in addition to their regional responsibilities also store CCP and certificate from the DTNAS needed for communication and request validity verification within the DTN network. NAS together with DTNAS implements the bundle layer that houses the Bundle Protocol (BP) needed for transportation of access control information.

6.2 Architecture Description

The architecture is designed to implement the bundle node of fig. 5 as DTNAS, NAS or End User in the respective private networks. It is based on traditional cryptography and designed to:

- Use a Common Communication Parameter (CCP) for communication during bundle transmission
- Provide security services on a hop-by-hop and end-to-end basis
- Support policy-based access control

The complexity of the node in terms of database size and computational capability decreases from DTNAS to End User. This is demonstrated in fig. 8 together with the relationship types of the architectural components.

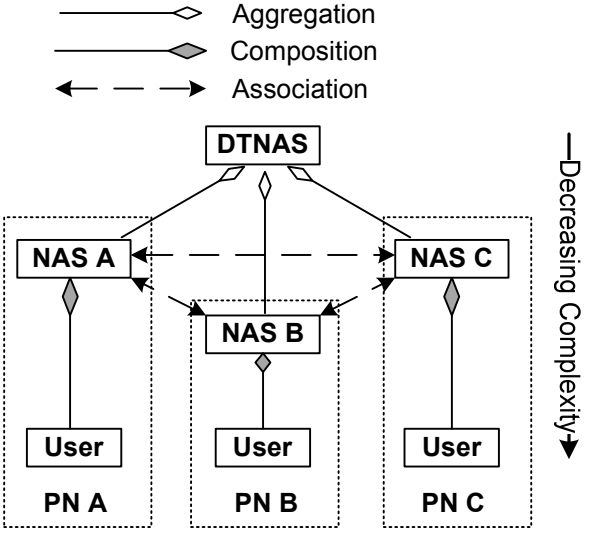

Fig. 8. Proposed Hierarchy and Relationship Type of Architectural Entities

The DTNAS and NAS of the various PNs are in aggregation relationship because NASs cannot operate in the DTN network without DTNAS, but can exist independently without DTNAS. NAS A, B and C are in association relationship because they hold a reference to one another through the certificate obtained from DTNAS after authentication during registration/service initialization. The End Users in the various PNs are in composition relationship with their respective NAS because the End Users cannot exist on their own since their existence in the various PNs is tied to the respective NASs. The following assumptions are considered:

- UNSC, DTNAS and NAS can generate their own key pairs
- UNSC and DTNAS cannot be compromised
- DTNAS and NAS provide UNSC with their public key and identity who in turn passes it on to designated entities together with a secret information for authentication purposes
- DTNAS has two public keys with the first one used during registration/service initialization and the second one after registration.
- Registration Request from NAS to DTNAS contains the identity of NAS and secret information obtained from UNSC while Registration Confirmation from DTNAS to NAS contains identity of DTNAS, secret information obtained from UNSC.
- All registered NAS will be in custody of certificate and CCP from DTNAS as well as the public key of DTNAS given after registration.

The Certificate and CCP are stored in the ASE of fig. 5 and the two phases considered for the description of the architecture are:

1. Registration/Service Initialization: During this phase, NAS sends registration request (regReq) to DTNAS which verifies the validity of request by comparing NAS identity and accompanying security information with its database content. If the credentials are genuine and other conditions met, DTNAS sends registration confirmation (regConf) to NAS accompanied by certificate and CCP. The public keys of the recipients are used by the communicating party for securing the message.

2. Data Exchange Phase: The security gateways (NASs) are assumed to be registered into the DTN network and in possession of the CCP, certificate from DTNAS, public key of DTNAS as well as individual key pairs. The CCP is used for BAB and other relevant keys for PIB and PCB. The use of CCP is intended to make communication within the DTN network free flowing. Any receiving node uses the CCP to access the BAB to authenticate itself and can only access the PIB and PCB if in position of the relevant keys. Since the BAB is the first security block to be accessed by the receiving node, we are of the opinion that the certificate from DTNAS should be housed in the BAB. Every receiving NAS confirms the DTNAS's identity and verify the signature in the accompanying certificate in the bundle with the public key in its custody. It also confirms the conformity of the action with the assigned role as well as the reputation of the sender. The receiving NAS accepts bundle custody if the sender is authenticated and authorized before proceeding with further bundle processing.

The sequence of action followed by DTNAS or NAS in verifying the validity of a request from another communicating party in either phase 1 or phase 2 is shown in

fig. 6. The architecture is designed to be dynamic and permits execution of phase 1 after the start of phase 2. This takes place either when an existing PN leaves the DTN network or new PN joins the DTN network.

6.3 Future Implementation

Future work will involve modeling the proposed lightweight hierarchical architecture in C++ and the validation of the result. In the course of the implementation, the following issues amongst others will be addressed:

- How can Mandatory Access Control (MAC) be implemented in DTN to address the identified limitations?
- Will combined implementation of Role-Based Access Control (RBAC) and MAC be feasible?
- What will be the nature of the CCP and content of the certificate?
- What will qualify an existing NAS for expulsion from the DTN network and what mechanism will be appropriate?

7 Conclusions

This paper proposed an access control framework for DTN environment and established the applicability of AAA architecture concept. We discussed security issues in DTN relating to resource consumption, as well as existing traditional access control solutions and their limitations. We identified desirable characteristics of an operational access control mechanism in the DTN environment and explored the DTN architecture to identify those features that will support the implementation of the AAA architecture concept.

In this paper, we have presented a lightweight hierarchical architecture for an intra-domain scenario and demonstrated how the three-party authentication model as well as the authorization push messaging sequence of the AAA architecture can be modified to suit the DTN environment. We compared the DTN bundle node structure with the generic AAA architecture to highlight the similarities between them and justify the suitability of the bundle node for AAA architecture concept implementation. We have proposed an access control sequence for the bundle node as well as how the architecture entities will relate in a hierarchical arrangement. Our framework will among other benefits prevent masquerading and modification attacks, reduce communication exchanges and overheads, support offline processing and empower the entities to make access control decisions internally.

This paper focuses mainly on design and gives an overview of the solution. The implementation and validation of the design in a delay/disruptive environment will be carried out in future work.

References

1. Farrell, S., Cahill, V.: Delay- and Disruption-Tolerant Networking. Artech House (2006) ISBN 1596930632
2. Cerf, V., Hooke, A., Torgerson, L., Durst, R., Scott, K., Fall, K., Weiss, H.: Delay-Tolerant Networking Architecture. IETF RFC 4838 (April 2007)

3. Fall, K.: A Delay-Tolerant Network Architecture for Challenged Internets. SIGCOMM, August 25-29 (2003)
4. Farrell, S., Cahill, V., Geraghty, D., Humphreys, I., McDonald, P.: When TCP Breaks: Delay- and Disruption Tolerant Networking. IEEE Internet Computing 10(4), 72–78 (2006)
5. Scott, K., Burleigh, S.: Bundle Protocol Specification. IETF RFC 5050 (November 2007)
6. Wood, L., Eddy, W., Holliday, P.: A Bundle of Problems. In: IEEE Aerospace Conference, Big Sky, Montana (2009)
7. Symington, S., Farrell, S., Weiss, H., Lovell, P.: Bundle Security Protocol Specification. Work in progress as an internet-draft, draft-irtf-dtnrg-bundle-security-07. September 9 (2009)
8. Fall, K., Farrell, S.: DTN: An Architectural Retrospective. IEEE Journal on Selected Areas in Communication (JSAC) 26(5), 828–836 (2008)
9. Farrell, S., Symington, S., Torgerson, L., Weiss, H., Lovell, P.: Delay-Tolerant Networking Security Overview. Work in progress as an internet-draft, draft-irtf-dtnrg-sec-overview-05, May 5 (2009)
10. Cruickshank, H., Pillai, P., Noisternig, M., Iyengar, S.: Security Requirement for Unidirectional Lightweight Encapsulation (ULE) Protocol. NWG RFC 5458 (March 2009)
11. Bhutta, M., Johnson, E., Ansa, G., Ahmed, N., Alsiyabi, M., Cruickshank, H.: Security Analysis for Delay/Disruption Tolerant Satellite and Sensor Networks. In: IWSSC 2009, Siena, Italy (September 2009)
12. Hu, V.C., Ferraiolo, D.F., Kuhn, D.R.: Assessment of Access Control Systems. National Institute of Standards and Technology, Interagency Report 7316 (September 2006)
13. House, T.C.: Client/Server Access: Satellite-ATM Connectivity Using Knowledge Management Approach. In: 4th International Conference on Information Technology: New Generations, Nevada, pp. 863–867 (2007)
14. Jiang, C., Li, B., Xu, H.: An Efficient Scheme for User Authentication in Wireless Sensor Networks. In: Advanced Information Networking and Applications Workshops, vol. 1, pp. 438–442 (May 2007)
15. Kim, K., Yang, J.: The Practical System Architecture for the Wireless Sensor Networks. In: International Conference on Multimedia and Ubiquitous Engineering, pp. 547–551 (April 2008)
16. Khakpour, A.R., Laurent-Maknavicius, M., Chaouchi, H.: WATCHMAN: An Overlay Distributed AAA Architecture for Mobile Ad Hoc Networks. In: The International Conference on Availability, Reliability and Security, pp. 144–152 (March 2008)
17. de Laat, C., Gross, G., Gommans, L., Vollbrecht, J., Spence, D.: Generic AAA Architecture. NWG RFC 2903 (August 2000)
18. Vollbrecht, J., Calhoun, P., Farrell, S., Gommans, G., Gross, G., de Bruijn, B., de Laat, C., Holdrege, M., Spence, D.: AAA Authorization Framework. NWG RFC 2904 (August 2000)
19. Nakhjiri, M., Nakhjiri, M.: AAA and Network Security for Mobile Access: Radius, Diameter, EAP, PKI and IP Mobility. John Wiley, Chichester (2005)
20. Blaze, M., Feigenbaum, J., Lacy, J.: Decentralized Trust Management. In: IEEE Symposium on Security and Privacy, May 6-8, pp. 164–173 (1996)
21. Bonatti, P., Duma, C., Olmedilla, D., Shahmehri, N.: An Integration of Reputation-based and Policy-based Trust Management, http://rewerse.net/publications/download/REWERSE-RP-2005-116.pdf
22. Blaze, M., Feigenbaum, J., Ioannidis, J., Keromytis, A.: The KeyNote Trust – Management System Version 2. NWG RFC 2704 (September 1999)

23. Chu, Y., Feigenbaum, J., LaMacchia, B., Resnick, P., Strauss, M.: REFEREE: Trust Management for Web Applications. Computer Networks and ISDN Systems 29(8-13), 953–964 (1997)
24. Ellison, C., Frantz, B., Lampson, B., Rivest, R., Thomas, B., Ylonen, T.: SPKI Certificate Theory. NWG RFC 2693 (September 1999)
25. Kagal, L., Finin, T., Joshi, A.: Trust-based Security in Pervasive Computing Environments. IEEE Computer Magazine 34(12), 154–157 (2001)
26. Blaze, M., Feigenbaum, J., Lacy, J.: The Role of Trust Management in Distributed Systems Security. In: Vitek, J. (ed.) Secure Internet Programming. LNCS, vol. 1603, pp. 185–210. Springer, Heidelberg (1999)