Automated Analysis of Internet Key Exchange Protocol v2 for Denial of Service Attacks

Hasmukh Patel[1] and Devesh C. Jinwala[2]
(Corresponding author: Hasmukh Patel)

Department of Computer Science & Engineering, L. C. Institute of Technology[1]
Mehsana-Unjha Highway, Bhandu, Mehsana, Gujarat, India
Department of Computer Engineering, Sardar Vallabhbhai National Institute of Technology[2]
Ichchhanath, Surat, Gujarat, India
(Email: hasu.patel@gmail.com)
(Received Nov. 24, 2012; revised and accepted July 17, 2013)

Abstract

The Denial of service (DoS) and Distributed Denial of Service (DDoS) attacks are aimed at maliciously consuming the available resources in computing systems to prevent genuine users from legitimately accessing them. These attacks can easily interrupt or disable targeted systems, so it is important for the system to detect and filter bogus connection requests as early as possible. Many common protocols TCP, HIP, SSL, etc., are vulnerable to DoS attacks. Until now, there has been no fit for all, generic solution to resist a DoS/DDoS attacks presented. An attractive alternative therefore is to investigate the approaches by which one can at least reduce the impact of the DoS/DDoS attacks. Our research work presented here focuses on the same.

We develop a formal model of Internet Key Exchange version 2 (IKEv2) protocol using formal specification language of Colored Petri Nets (CPNs) to analyze the protocol for DoS attacks. IKEv2 is a member of the IPSec protocol suite and establishes a security association that includes secret information between source and destination. IPSec provides security services to applications viz. VPN, remote login, email, file transfer etc. Till date no automatic formal analysis of IKEv2 protocol is attempted for DoS attacks, hence we choose IKEv2 protocol to illustrate automatic analysis for DoS attacks. We use simulation approach of CPNs to analyze the protocol for DoS attacks. We analyze the processing cost and memory cost to carry out DoS attacks in IKEv2. In addition, we measure the strength of the protocol against DoS attacks using different experiments in CPNs.

Keywords: Colored petri nets, denial of service attacks, Internet key exchange protocol version2

1 Introduction

With the rapid growth of the Internet and the consequent proliferation of the Web-enabled services in every aspect of human activities, it has become all the more challenging to ensure the security as well as availability of the services offered. One of the potent threats to the security and availability of the Web Services is a Denial of Service (DoS) attack that can be orchestrated by an adversary even without any significant and sophisticated armory and skills. Hence, it is essential to investigate the means and technologies by which such attacks can be thwarted. In case such attacks cannot be thwarted then it is necessary to investigate how the consequences thereof can be minimized to the extent possible. Our research work described herein focuses on the issues associated with the analysis of the DoS attacks and minimizing the consequences thereof.

DoS attacks can broadly classified into logical attacks and resource exhaustion attacks. The logical attacks are kind of smart attacks. To mount logical attacks, the attacker should find out the vulnerabilities in an application installed on or protocols use by targeted system/service provider. In resource exhaustion attacks, an attacker tries to exhaust the resources viz. CPU, memory or network bandwidth of a service provider [1, 14]. The ultimate goal of the attacker is to prevent a genuine user from using the services. Hence, DoS attacks are dangerous and devastating attacks.

The key exchange protocols used to establish a shared key to make secure communication possible. They use expensive cryptographic operations to derive the shared key and to transfer it securely. Hence, the key exchange protocols are vulnerable to DoS attacks. Therefore, it is very crucial to verify the key exchange protocols for availability property. Our focus is to analyze the strength of key exchange protocols against DoS attacks.

2 Motivation

When we design computer systems to pursue security, availability should not be compromised. One of the ways to compromise availability is DoS attacks. Protocols viz. HIP [16], SSL [17], JFK [11, 15] etc. were designed very carefully, even though they are found vulnerable to DoS attacks. Hence, we emphasize that the formal analysis

should model and verify confidentiality, integrity as well as availability property of the protocols.

Designing protocols to withstand DoS attacks is a very complex task [15]. To the best of our knowledge, still there is no guaranteed technique to differentiate attacker's bogus request from genuine user request. Authentication has been used to authenticate the user and allow them to connect to the service provider. However, authentication itself is very resource expensive operation. An attacker may take advantage of this and fire many requests to mount a resource exhaustion attack. Gradual authentication [12] can be applied to increase the level of authentication at each step of the protocol. Even though, the protocols with the gradual authentication need to analyze formally for DoS attacks.

The framework pursued to analyze protocols for DoS attacks is Meadows cost-based framework [12]. It is a basic framework and there is a scope for an improvement. Tritilanunt et al. improved the Meadows framework with refinement in cost calculation [16, 17]. They also model and analyze the HIP protocol for DoS attacks using CPNs. However, they only use computational cost to analyze the protocol.

Internet Key Exchange version 2 (IKEv2) is a simple, efficient and secure key exchange protocol [10]. IPSec provides security services to applications viz. VPN, remote login, email, file transfer etc. Hence, it is very crucial to verify the IKEv2 protocol for DoS attacks. Rui Jiang et al. proposed efficient and secure key exchange protocol to overcome the security shortage of IKE protocol [9]. Cas Cremers presented modeling and analysis of IKEv1 and IKEv2 protocols using Scyther, a security protocol verifier tool, for secrecy and authentication properties only [4]. However, to the best of our knowledge, till date there has been no automatic and formal analysis of IKEv2 for DoS attacks is attempted. Hence, it is very essential to verify IKEv2 protocol for DoS attacks. Therefore, in this paper, we analyze IKEv2 protocol and examine processing and memory cost that leads to resource exhaustion attacks.

The tools viz. Scyther, Proverif, Avispa/Avantssar, NRL, Colored Petri Nets (CPNs) etc. developed for analyzing security protocols using formal methods. CPNs, general-purpose verification tool, is more suitable and beneficial in the analysis and verification of cryptographic protocols [7, 8]. It can be used to analyze the behavior of the modelled system using simulation, state space methods and model checking [7]. In this paper, by adopting idea of Tritilanunt's [16] refined processing cost calculation of Meadows framework [12], we develop a formal model of IKEv2 protocol using CPNs to analyze for DoS attacks. We use a simulation approach provided in CPN Tools to achieve a formal analysis. Our simulation provides an accurate cost estimation of processing as well as memory of protocol execution comparing among principals. In addition to that, we measure the tolerance of IKEv2 protocol under DoS attacks.

The contributions of this paper are.

- Formal modeling and automatic analysis of IKEv2 protocol using CPNs (Section 3 and Section 4);
- Identification of three types of attackers to analyze IKEv2 protocol (Section 3);
- As per idea of Meadows framework, processing and memory cost analysis at each step of protocol (Section 4);
- Performance measure to check tolerance of IKEv2 protocol under DoS attacks (Section 4).

The remaining paper is organized as follow. In Section 3, we discuss modeling of IKEv2 protocol and types of attackers considered for analysis. In Section 4, we analyze the IKEv2 protocol for computational and memory cost. In Section 5, we describe related work to verification of protocols for DoS attacks using CPNs. We conclude our work in Section 6.

3 Modeling

In this section, we model the IKEv2 protocol to analyze for DoS attacks using CPN Tools. We describe the types of attackers identified for analysis of IKEv2 protocol. Table 1 gives the message sequence of IKE v2 protocol.

Table 1: IKEv2 protocol

$$A \rightarrow B: HDR_1, SA_{a1}, g^{XA}, N_A$$
$$B \rightarrow A: HDR_2, SA_{b1}, g^{XB}, N_B$$
$$A \rightarrow B: HDR_3, \{ID_A, ID_B, AUTH_A, SA_{a2}, TS_a, TS_b\}_{SK}$$
$$B \rightarrow A: HDR_4, \{ID_B, AUTH_b, SA_{b2}, TS_a, TS_b\}_{SK}$$

Where

$$AUTH_a = \{SA_{a1}, g^{XA}, N_A, N_B, prf_{SK_{pa}}(ID_A)\}_{SK(A)}$$
$$AUTH_b = \{SA_{b1}, g^{XB}, N_B, N_A, prf_{SK_{pb}}(ID_B)\}_{SK(B)}$$

We describe IKEv2 protocol in the annotated Alice-Bob specification in Table 2. The purpose of Alice-Bob specification is to give the details of operations in execution of protocol on initiator as well as responder side. Table 3 presents the cost of some specific cryptographic algorithms, which are part of IKEv2 protocol. The costs of operations are from the cryptographic protocol benchmarks by Wei Dai [5].

3.1 Attacker Types

By adopting idea of Tritilanunt's [16], we identify three types of attackers to analyze IKEv2 protocol that follow the protocol execution and have a limited capability to spoof the messages.

Attacker Type 1: Attacker Type 1 randomly chooses the components of first message, and then takes no further action. The intention of this type of attacker is to flood the responder using spoofed IP addresses.

Table 2: Annotated Alice-Bob specification of IKEv2

$A \rightarrow B$	$\text{createexp}_1(g^X A), \text{computenonce}_1(N_A) \parallel g^{XA}, N_A \parallel$ $\text{verifygroup}(g^X A), \text{accept}_1$
$B \rightarrow A$	$\text{createexp}_2(g^X B), \text{computenonce}_2(N_B) \parallel g^{XB}, N_B \parallel$ $\text{verifygroup}(g^X B), \text{accept}_2$
$A \rightarrow B$	$S_1 = \text{generatesign}_1(N_A, N_B, g^{XB}, g^{XB}, ID_A, SA_a 1)$, $Enc_1 = \text{encrypt}_1(K, \{ID_A, S_1, SA_{a1}\})$, $D_1 = \text{generatemac}_1(K, Enc_1) \parallel Enc_1, D_1 \parallel$ $\text{generatedh}_2(g^{AB}), K = \text{computekey}_2(N_A, N_B, g^{AB})$, $\text{verify}_1(D_1 = \text{generatemac}_2(K, Enc_1)), \text{decrypt}_1(K, Enc_1)$, $\text{verifysign}_1(S_1), \text{accept}_3$
$B \rightarrow A$	$S_2 = \text{generatesign}_2(N_A, N_B, g^{XA}, g^{XB}, ID_B, SA_{b2})$, $Enc_2 = \text{encrypt}_2(K, \{ID_B, S_2, SA_{b2}\})$, $D_2 = \text{generatemac}_3(K, Enc_2)$ $\parallel Enc_2, D_2 \parallel \text{verify}_2(D_2 = \text{generatemac}_4(K, Enc_2))$, $\text{decrypt}_1(K, Enc_2), \text{verifysign}_1(S_2), \text{accept}_4$

Table 3: Computational cost of CPU usage of specific algorithm

Key Exchange	**Megacycle/ Operation**	**Symmetric Crypto**	**Cycles/ Bock**
Diffie-Hellman Key pair generation	1.51	DES	15320
Diffie-Hellman Key Agreement	2.16	AES/CBC (128-bit key)	1041
Public Key Crypto	**Megacycle/ Operation**	**Hash**	**Cycles/ Bock**
RSA Signature	2.71	HMAC/MD5	932
RSA Verification	0.13		

Attacker Type 2: Attacker Type 2 follow the protocol for first message. Randomly chooses the components to create the third message. The intention of this type of attacker is to make responder to consume resources for expensive operations like Diffie-Hellman key generation and encryption.

Attacker Type 3: Follow the protocol up to third message and then takes no further action. Computation includes generation of encryption and authentication key, signature generation and encrypting the message. The intention of this type of attacker is to make responder to verify the signature and sign the message to generate the response of third message.

3.2 Modeling using Colored Petri Nets for IKEv2 protocol

We use CPNs to model IKEv2 protocol. Figure 1 shows the main page of hierarchical CPNs for IKEv2 protocol. The model consists of three main components. They are initiator, network and responder. There is a subpage for generation and processing of each message from the main page. Figure 2 shows responder subpage to process the received message 1 and generate message 2. The color of token contains three kinds of data includes name of component, processing cost and memory cost.

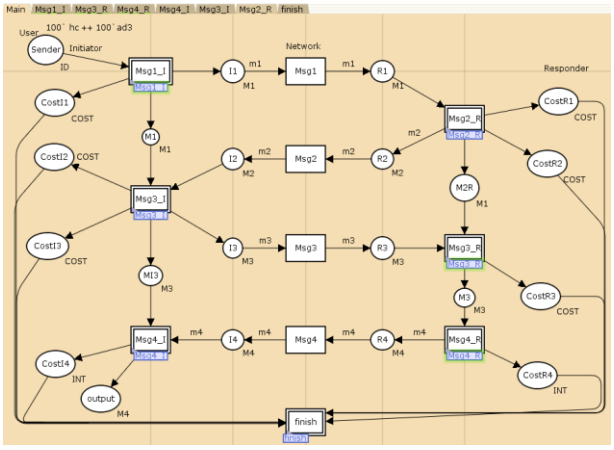

Figure 1: Main page of hierarchical Coloured Petri Nets of IKEv2

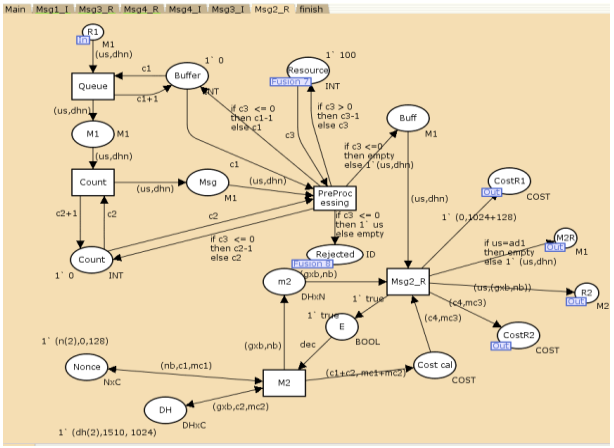

Figure 2: Responder sub page - processing message 1 and generate message2

4 Analysis

In this section, we analyze the IKEv2 protocol. We consider three parameters for analysis. First is processing cost of cryptographic operations involved in protocol execution. Second is memory cost for components of protocol require to store in memory as part of protocol execution. We measure and analyze unbalanced computation and memory cost. Third is to measure the tolerance of IKEv2 protocol under different DoS attacks scenarios.

4.1 Processing Cost Analysis

We simulate the model of IKEv2 protocol for honest client and three types of attackers identified in Section 3. Table 4 shows the computational cost incurred between different

types of attackers and responder. In case of honest client and attacker Type 1, the cost of initiator and responder are same.

Table 4: Comparison of Initiator and Responder computational cost for IKE v2

Protocol	Initiators	Initiator Cost	Responder Cost
IKE v2	Honest Client	6544	6544
	Attacker Type1	1510	1510
	Attacker Type2	1511	3673
	Attacker Type3	6398	6544

Table 5: Comparison of Initiator and Responder memory-cost for IKE v2 protocol

Protocol	Initiators	Initiator Cost(bits)	Responder Cost(bits)
IKE v2	Honest Client	3744	3744
	Attacker Type1	1152	2304
	Attacker Type2	1152	3744
	Attacker Type3	3744	3744

IKEv2 protocol uses cookie when it encounter more than pre-configured number of half-open request packets. If many IP-spoofed requests are received in a short time, IKE v2 protocol send cookie require message to one of the sender and ignore other messages [10]. This prevents flooding attacks at message1.

Attacker Type 2 randomly chooses the message component hence the cost of creating the message is almost negligible. On the other side the responder has to perform expensive operations to calculate Diffie-Hellman key and other required keys before checking the message correctness. Hence, attacker Type 2 may lead to resource exhaustion at responder. Attacker Type 3 consuming highest amount of resource among all, but the ratio of the resource consumption of responder to the attacker is less than attacker Type 2. Hence, we conclude that attacker Type 2 is most effective attacker compare to other types of attackers.

4.2 Memory Cost Analysis

Table 5 shows the memory requirement of the IKEv2 protocol in execution for honest client and three types of identified attackers in Section 3. As per the recommendation of IKEv2 specification [10] minimum nonce size is 128 bits, Diffie-Hellman key size is 1024 bits, encryption key and MAC key size are 256 bits and 160 bits respectively. Diffie-Hellman key size depends on the group selected to establish a security association. The key size of an algorithm depends on the selection of cryptographic suite in process to establish a security association. We consider the minimum key size for components of protocol in analysis.

Stateless connection [3] and gradual authentication [12] are techniques proposed to prevent the memory exhaustion attacks. However, the responder cannot be a complete stateless. Components like nonces, encryption keys etc. need to be stored at responder for authentication of connection.

Table 5 show that attacker Type 1 may lead to memory exhaust; however, IKEv2 use cookie when number of half-open connection request exceeds pre-configured number.

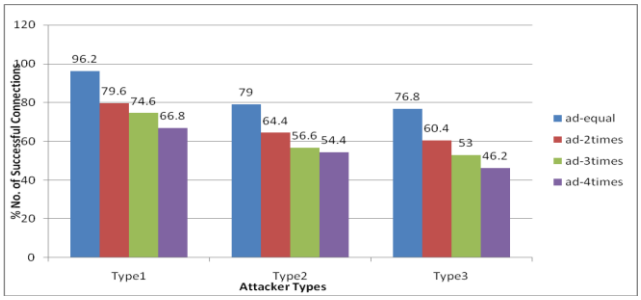

Figure 3: DoS attack tolerance of IKEv2 protocol

Once first message is received correctly and response to the message generated, half-open connection counter decremented and state is created at responder side. We can see from Table 5 that there is a large difference in memory requirement of attacker Type 2 and responder. There is no way to detect that a message received is spoofed until Diffie-Hellman key and other required keys are calculated to authenticate the request, hence it may lead to a memory exhaust. Attacker Type 2 spoofs the message components; hence, it does not require to store the message components. Memory requirements of attacker Type 3 and responder are same. Therefore, Attacker Type 2 is most effective attacker among all.

4.3 DoS Attack Tolerance of IKEv2 Protocol

We set up an experiment to measure the tolerance of IKEv2 protocol for DoS attacks under different scenarios. We make a pair of honest client with each type of attacker. We measure the number of successful connections of the honest client in case of DoS attacks by each type of attacker. To measure the tolerance of IKEv2 protocol under DoS attacks, we increase number of requests of attacker by two times, three times and four times and note the number of successful requests of the honest client in each case. The overall result is shown in Figure 3.

From Figure 3, we note that, number of successful requests of the honest client decreasing as we go from attacker Type 1 to Type 3. In case of attacker Type 3, number of successful connections of honest client is least. This is because the requests from attacker Type 3 consume the highest amount of resources of responder among all attackers. The ratio of resource consumption of responder to resource consumption of attacker Type 2 is higher than that of attacker Type 3. Table 4 and Table 5 confirm the same. Figure 3 shows the percentage number of successful connections of honest client in twelve different experiments. We conclude from Figure 3 that attacker Type 3 is most effective to interrupt the performance of the responder.

5 Related Work

The purpose of this section is to provide work related to the analysis of security protocol for DoS attacks using CPN Tools.

CPNs has been used for modeling and analysis of security protocols since many years. CPNs is very effective in the analysis and verification of cryptographic protocols [6, 7, 8]. Yang et al. analyzed Andrew secure RPC protocol for secrecy and authentication using CPNs [19, 20]. Issam Al-Azzoni et al. presented technique to model and analyze protocol using CPNs with implementation of TMN protocol [2]. The authors have also integrated generic intruder model and introduced techniques to reduce size of occurrence graph.

There are also efforts to analyze the protocol for DoS attacks using CPN Tools. Jin et al. has used CPN Tools for modeling and analysis of JFK protocol for DoS attacks [18]. Tritilanunt et al. [16, 17] have developed timed CPNs model by adopting the key idea of Meadows framework [12, 13] and incorporating refined cost calculation for SSL and HIP protocols to analyze for DoS attacks. The authors have also calculated the number of successful connections of legitimate user under different attacks strategies.

To the best of our knowledge, there is no implementation of IKEv2 protocol model using CPNs to analyze for DoS attacks. Therefore, we model the IKEv2 protocol using hierarchical CPNs and analyze for processing cost as well as memory cost. In addition to that, we measure the strength of protocol against DoS attacks under different scenarios of DoS attacks.

6 Conclusion and Future Work

When we design computer systems to pursue security, availability should not be compromised. One of the ways to compromise availability is DoS attacks. It is essential to investigate a formal analysis technique that can at least reduce the impact of the DoS attacks.

In this paper, we have developed formal specification of IKEv2 protocol in CPNs. We analyzed IKEv2 protocol for processing and memory cost. We use simulation approach of CPN Tools to measure the tolerance of the protocol against DoS attacks under different scenarios.

In future work, we plan to extend the protocol model by integrating more powerful intruder model. The main issue is to identify the attacker actions and to assign the cost to those actions. Another area to explore is to design and implement a generic model to verify protocols for availability property with goal to improve protocol against DoS attacks. Our eventual goal of this work is to analyze protocols for DoS attacks and strengthen protocols against DoS attacks.

References

[1] CERT, *Denial of Service Attacks*, 3 May 2010. (www.cert.org/tech_tips/denial_of_service.html)

[2] I. Al-Azzoni, D. G. Down, and R. Khedri. "Modeling and verification of cryptographic protocols using coloured petri nets and design/CPN," *Nordic Journal of Computing*, vol. 12, no. 13, pp. 201-228, June 2005.

[3] T. Aura and P. Nikander. "Stateless connections," in *Proceedings of the First International Conference on Information and Communication Security (ICICS '97)*, LNCS 1334, pp. 87-97, Springer-Verlag, 1997.

[4] C. Cremers, "Key exchange in IPsec revisited: Formal analysis of IKEv1 and IKEv2," in *16th European Symposium on Research in Computer Security (ESORICS-2011)*, pp. 315-334, Leuven, Belgium, Sep. 12-14, 2011.

[5] W. Dai, Crypto++ 5.2.1 Benchmarks, 2009. (http://www.cryptopp.com/benchmarks.html)

[6] E. M. Doyle, *Automated Security Analysis of Cryptographic Protocols using Coloured Petri Net Specification*, Master of Science Thesis, Department of Electrical and Computer Engineering, Queen's University, Ontario, Canada, 1996.

[7] K. Jensen, L. M. Kristensen, L. Wells. "Coloured petri nets and CPN tools for modeling and validation of concurrent System," *International Journal Software Tools Technology Transfer*, vol. 9, pp. 213-254, 2007.

[8] K. Jensen, "An introduction to the theoretical aspects of colored petri nets," in *Workshop on the Applicability of Formal Models*, pp. 230-272, 1994.

[9] R. Jiang, A. Hu, and J. Li, "Formal protocol design of ESIKE based on authentication tests," *International Journal of Network Security*, vol. 6, no. 3, pp. 246-254, 2008.

[10] C. Kaufman, P. Homan, Y. Nir, P. Eronen, *Internet Key Exchange Protocol Version 2 (IKEv2)*, RFC 5996, Sep. 2010. (http://www.rfc-editor.org/info/rfc5996)

[11] L. Kuppusamy, J. Rangasamy, D. Stebila, C. Boyd, and J. N. Gonzalez. "Towards a provably secure DoS-Resilientkey exchange protocol with perfect forward secrecy," in *Indocrypt*, pp.379-398, Springer-Verlag, Chennai, India, 2011.

[12] C. Meadows. "A cost-based framework for analysis of denial of service networks," *Journal of Computer Security*, vol. 9, no. 1, pp. 143-164, 2001.

[13] C. Meadows. "A formal framework and evaluation method for network denial of service," in *Proceedings of 12th IEEE Computer Security Foundations Workshop (CSFW)*, pp. 4-13, 1999.

[14] J. Smith, S. Tritilanunt, C. Boyd, J. Gonzalez Nieto, and E. Foo. "Denial of service resistance in key establishment." *International Journal of Wireless and Mobile Computing*, vol. 2, no. 1, pp. 59-71, 2007.

[15] J. Smith, J. M. Gonzalez Nieto, and C. Boyd. "Modeling denial of service attacks on JFK with Meadows's cost-based framework," in *4th Australasian Information Security Workshop*, vol. 54, pp. 125-134, 2006.

[16] S. Tritilanunt, C. Boyd, J. M. Gonzalez Nieto, and E. Foo. "Cost-based and time-based analysis of DoS-

resistance in HIP," in *Proceedings of the Thirteeth Australasian Computer Science Conference*, pp. 191-200, Ballarat, Australia, 2007.

[17] S. Tritilanunt, C. Boyd, E. Foo, and N. Gonzalez Juan. "Using coloured petri nets to simulate DoS-resistant protocols," in *7th Workshop and Tutorial on Practical Use of Coloured Petri Nets and the CPN Tools*, Denmark, Aarhus, 2006.

[18] J. Wei, G. Su, and M. Xu. "An Integrated Model to Analyze Cryptographic Protocols with Colored Petri Nets," *11th IEEE High Assurance Systems Engineering Symposium*, IEEE, pp. 457 -460, 2008.

[19] Y. Xu and X. Xie. "Modeling and analysis of security protocols using colored petri nets," *Journal of Computers*, vol. 6, vo. 1, Academy Publisher, Jan. 2011.

[20] Y. Xu and X. Xie. "Modeling and analysis of authentication protocols using coloured petri nets," in *3rd International Conference on Anti-counterfeiting, Security, and Identification in Communication*, pp. 443-448, 2009.

Hasmukh Patel is serving as an Assistant Professor in Computer Science & Engineering Department with Laljibhai Chaturbhai Institute of Technology, Bhandu (India). His major areas of interests are verification of security protocols, Information and Network Security.

Dr. Devesh Jinwala is serving as an Associate Professor in Computer Engineering with Sardar Vallabhbhai National Institute of Technology, Surat (India). His major research areas of interests are Information Security in general and that in Resource Constrained Environments, specifically; Algorithms & Computational Complexity and Using Ontologies in Software Requirements and Specifications.