INTERNET-DRAFT Intended Status: Standards Track Expires: January 30, 2019 Annu NIT Delhi K.Verma NIT Delhi

August 3, 2018

ike for wsn security draft-annu-t2trg-ike-for-wsn-security-00.txt

Status of this Memo

This Internet-Draft is submitted to IETF in full conformance with the provisions of <u>BCP 78</u> and <u>BCP 79</u>.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

The list of current Internet-Drafts can be accessed at http://www.ietf.org/lid-abstracts.html

The list of Internet-Draft Shadow Directories can be accessed at http://www.ietf.org/shadow.html

Copyright and License Notice

Copyright (c) 2018 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to <u>BCP 78</u> and the IETF Trust's Legal Provisions Relating to IETF Documents (<u>http://trustee.ietf.org/license-info</u>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License. Annu, K.Verma Expires January 30,2019

[Page 1]

Abstract

This document specifies an internet key exchange(ike) protocol for wireless sensor network.IKE is a component of IPsec used for performing mutual authentication and establishing and maintaining security associations. This document preassumed that readers are familier with basic concept of sensor network.

Table of Contents

<u>1</u>	Introduction $\ldots \ldots 2$
<u>2</u>	Terminology
<u>3</u>	IKE Introduction
<u>3.1</u>	Ike Message Flow
<u>4</u>	IKE Protocol Variations $\underline{4}$
<u>5</u>	Solution
<u>6</u>	Comparision Between Protocols Used
7	IANA Consideration $\ldots \ldots \underbrace{9}$
<u>8</u>	Security Considerations
<u>9</u>	Conclusion
<u>10</u>	References
<u>11</u>	Acknowledgement
	Authors' Addresses

1 Introduction

In wsn providing secure communication between two nodes or between nodes and BS is major issue. This document helps in identifing faulty nodes and separate them from the rest of the network and create tunnel for secure communication , so that the acquired data remains reliable. So for secure communication and protecting network from vulnerable node we used ike.

2 Terminology

- 2.1 SA: Security Association
- 2.2 encp: Encryption
- 2.3 DH: Diffie-Hellman key exchange
- 2.4 Auth: Authentication
- 2.5 WSN: Wireless Sensor Network
- 2.6 IKE: Internet Key Exchange
- 2.7 Node: Sensor nodes
- 2.8 BS: Base Station
- 2.9 Reci: Receiver

Annu, K.Verma Expires January 30,2019

3 Ike intoduction

Ike is used in conjunction with IPsec to dynamically and automatically create SA.IKE performs mutual authentication between two parties and establishes an IKE SA that includes shared secret information that can be used to efficiently establish SAs for Encapsulating Security Payload (ESP) [RFC 4303] and/or Authentication Header (AH) [RFC 4302] and a set of cryptographic algorithms to be used by the SAs to protect the traffic that they carry. for more details see [RFC 7296].

3.1 Ike message flow

IKE message flow always consists of a request followed by a response.It is the responsibility of the requester to ensure reliability. If the response is not received within a timeout interval, the requester needs to retransmit the request

3.1.1 IKE phase one

The first request/responce of an IKE session negotiates security parameters for the IKE_SA, sends nonces, and sends Diffie-Hellman values.

++	++
sender	receiver
++	+++
 sender sends its SA to rec +	
encp/hash methods 	
receiver returns its selec of methods < 	
 receiver and sender excha DH public keys <	I
sender and receiver have authenticated each other <	
sender and receiver starte exchanging data <	

| | + + fig.1 IKE phase one process

Annu, K.Verma Expires January 30,2019 [Page 3]

3.1.2 IKE phase two:

The second request/response (IKE_AUTH) transmits identities, proves knowledge of the secrets corresponding to the two identities, and sets up an SA for the first AH and/or ESP CHILD_SA.

++ +-	+
sender r	eceiver
++ +-	-++
sender sends its ipsec SA	
to recei	
+>	
recei. send its ipsec SA to	
sender	
<	- +
<pre>ipsec tunnel is created and</pre>	
<pre> all data is encrypted</pre>	
<>	
+	+

fig.2 IKE phase two process

4 IKE protocol variations :

IKE uses RSA as public key cryptography algorithm that is based on Diffie-Hellman (DH) see 9.2[1] key exchange which is very heavy, in term of arithmetic operations, for very constrained resources devices such as the case for WSNs. So that's why we use other protocols for encp/auth/integrity instead of RSA and DH. some of these protocols are: a) LEAP

- b) SPINS
- c) Minisec
- d) Tinysec

Annu, K.Verma Expires January 30,2019

4.1)LEAP(Localized Encryption And authentication Protocol): key management protocol for Sensor Networks designed to support secure communications in these networks. It provides authen and confidentiality.

LEAP has following features:

- 1)LEAP provides four types of keys for each sensor node- an individual key shared with the base station, a pairwise key shared with other Sensor Node, a Clustered key shared with multiple neighbouring nodes, and a group key shared by all nodes in the network.
- 2)LEAP includes use of one-way key chains for local broadcast authentication.
- 3)Key sharing mechanism of LEAP supports in- network processing Thus LEAP can prevent or make it complex to attack nodes on the sensor network.

+	-+		-+-		-+		- +		+					+
		е	Ι	f	Ι		Ι		I					
		n		r		m		0				а		
p		С		е		а		V			k	g		
r		r		S		С		е			е	r		
0		У		h				r			У	е		
t		р		n		u		h				е		
0		t		е		S		е				m		
C		i		S		е		а				е		
0		0		S		d		d				n		
1		n										t		
+														+
leap		ye	s	no		yes	Va	ariab	le	рі	re-	depl	oyed	1
							1		I	١	/ar	iabl	е	
+	-+		-+-		-+		- +		+					+

fig.3 LEAP PROTOCOL

Annu, K.Verma Expires January 30,2019

[Page 5]

- 4.2) SPINS(Security Protocols for Wireless Sensor Networks): SPINS see 9.2[2] consists of two main protocol:
 - 1)SNEP: In SNEP, plain text block is encrypted with a counter using CTR encryption algorithm. The counter is not included in the message.Each message has a MAC computed with CBC-MAC see 10.2[4] nalgorithm in the encrypted data. The MAC is computed once for each package
 - SNEP has following advantages:
 - a.SNEP uses a shared counter so it need not to be transmitted with the message.
 - b.It adds only 8 bytes to a message.
 - c.It offers following kind of security to the data in transit Semantic Security Data Authentication **Replay Protection** Weak Freshness Low communication overhead
 - 2) mueTESLA: In this protocol a node stores the packet in the buffer till the key is disclosed. The time when the key is disclosed , the base-station broadcasts verification key to all the receivers, which the node can use to authenticate the packet stored in its buffer. Each MAC key is a sequence of keys generated by one way function F. The sender chooses last key Kn and repeatedly applies F to compute the keys Ki = F(Ki+1)

+	+		-+-		- + -		- + -		+ -			+
		е		f								
		n		r		m		0			а	
p		С		е		а		V		k	g	
r		r		S		С		е		е	r	
0		У		h				r		У	е	
t		р		n		u		h			е	
0		t		е		S		е			m	
C		i		S		е		а			е	
0		0		S		d		d			n	
1		n									t	
+												+
spi	ns	ye	s	yes	5	/es	8	8 Byt	es s	ymm	etri	c
										del	ayed	
+	+		-+-		- + -		- + -		+ -			+

fig.4 SPINS PROTOCOL

Annu, K.Verma Expires January 30,2019

[Page 6]

4.3) Minisec:

MiniSec see 9.2[3] is a secure network layer protocol that have lower energy consumption than TinySec but level of security matches with that of Zigbee. It uses offset Codebook Mode(OCB) as its block cipher mode of operation. Two passes are required for secrecy and authentication.OCB mode for faster MAC + ciphertext.

+	+		-+		+	+	-+-			+
	I	е	I	f						
		n		r	m	0			а	
p	Ι	С		е	a	∧		k	g	I
r		r		S	C	e		е	r	
0	Ι	У		h		r		у	е	
t	Ι	р		n	u	h			е	- 1
0	Ι	t		е	S	e			m	I
C	Ι	i		S	e	a			е	I
0	Ι	0		S	d	d			n	
1	Ι	n							t	
+										+
mini	Ι	ye	s	yes	yes	4+3Byte	es	an	у	
sec						1				
+	+		-+		+	+	-+-			+

fig.5 MINISEC PROTOCOL

4.4) Tinysec: It provides all the services provided by SNEP like authentication, message integrity, confidentiality and replay protection.Major difference is that no counters are used in TINYSEC.

Two variants of TINYSEC are available TINYSEC-AE(authentication Encryption) TINYSEC-Auth(Authentication Only)

+	-+	+		+	+ -		+ -			+
	€) ș	f	Ι			Ι			
	r	ן ו	r	m		0			а	
p	0	:	е	a		V		k	g	
r	r	-	S	c		е		е	r	
0)	/	h			r		У	е	
t)	n	u		h			е	
0	t	:	е	s		е			m	
C	i	i	S	e		а			е	
0	0	0	S	d		d			n	
1	r	ן ו							t	
+										+
tiny	13	/es	no	ye	s 4	4 Byt	es	an	У	

|sec | | | | | | | +----+

fig.6 TINYSEC PROTOCOL

Annu, K.Verma Expires January 30,2019

[Page 7]

INTERNET DRAFT

ike for wsn security August 3, 2018

5 Solutions:

As we already discribed in <u>section 4</u> we have different protocols for encp, auth, integrity and freshness in wsn. So during the phase one of the ike sender and receiver shoule aggred upon one of the protocols stated above. Sender send its SA proposal to receiver and after that receiver reply with the selection of methods. Then sender and receiver auth each other. so with this authentication between sender and receiver the problem which we discussed in section 1 (faulty node identification) is resolved bcoz before communication started each node needed to be authenticated. After completion of phase 1[fig 1] , phase 2 [fig 2] started in that phase also sender and receiver exchage their SA. when the exchange of SA is completed then a secured tunnel is created between twop nodes. nodes can be either two sensors or may be sensor and base station. And the communication through this tunnel is secure.

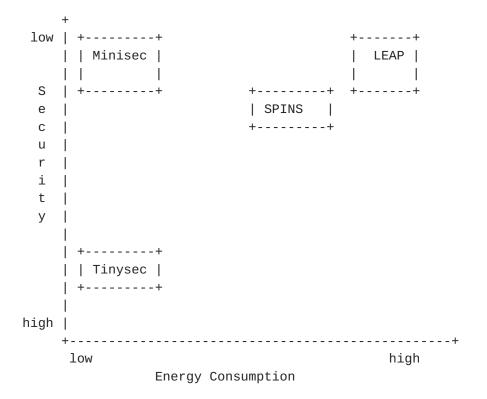
+	+	+	-+
Protected	tunnel mode SA	Protected	
Endpont	<>	Endpoint	
I			
I			
+	+	+	-+

fig.7 Tunnel Created

6 comparision between protocols used:

+	+	+	+	++
	 LEAP 	 SPINS 	 Tinysec 	Minisec
Overhead (Bytes)	Variable 	8 	4	4+3
Encryption +	yes 	yes 	yes 	yes
Mac Used +	yes 	yes 	yes 	yes
Freshness +	no 	yes 	no 	yes
Key Aggrement		symmetric Delayed	Any 	Any

Annu, K.Verma Expires January 30,2019 [Page 8]



7 IANA Considerations

Nil

8 Security considerations

Generally IKE is protocol of ipsec protocol suite. IKE provides the following benefits for IPsec: a)Automatically negotiates IPsec parameters. b)Performs DH exchanges to calculate shared keys, making sure each SA has a key that is independent of other keys, encrypt keys. c)Automatically negotiates SAs when the sequence number in the AH or ESP header overflows, making sure IPsec can provide the anti-replay service by using the sequence number.

In our proposed method we used Ike for wsn security and auth for the solutions we discussed in sec.5 we can use any protocol. At the time of SA sender and receiver choose energy efficient and secure protocol as comparision discussed in <u>section 6</u>.

Annu, K.Verma Expires January 30,2019 [Page 9]

9 Conclusion

This document is mainly focussed over the security in wsn. Sensor nodes are constraints in term of size, power consumption, memory processing power. Due to limited battery and processing power. This document implemented IKE with energy efficient protocls used for sensor network instead of RSA and DH as discussed in sec 4. With the scheme proposed by this document we can encrypt data and auth nodes and create a secured tunnel for further communication.

10 References

10.1 Normative References

[RFC 4302] https://www.rfc-editor.org/rfc/pdfrfc/rfc4302.txt.pdf [RFC 4303] https://www.rfc-editor.org/rfc/pdfrfc/rfc4303.txt.pdf [RFC 7296] C.Kaufman,Ed. "Internet Key Exchange(IKEv2)Protocol"

10.2 Informative References

- [1] http://www.cse.nd.edu/~cseprog/proj00/proceedings.pdf#page=67
- [2] https://link.springer.com/content/pdf/ 10.1023%2FA%3A1016598314198.pdf
- [3] https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=4379708
- [4] https://www.rfc-editor.org/rfc/pdfrfc/rfc3610.txt.pdf

11 Acknowledgement:

This document is prepared for M. Tech 2nd year Major Project in National Institute of Technology, Delhi.

Annu, K.Verma Expires January 30,2019

[Page 10]

Authors' Addresses

Annu M.Tech Student Department of Computer Science & Engineering National Institute of Technology, Delhi Narela, Delhi-110040,INDIA

Phone: +91-9729995908 EMail: 172211003@nitdelhi.ac.in

Karan Verma Assistant Professor Department of Computer Science & Engineering National Institute of Technology, Delhi Narela, Delhi-110040,INDIA

Phone: +91-7568169258 EMail: karan.verma.phd@gmail.com

Annu, K.Verma Expires January 30,2019

[Page 11]