Volume 7, Issue 5, May 2017 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Modification of WIMAX Self –Organized Efficient Authentication and Key Management (SEAK) Security Protocol

Salih Yasien Salih[1], Amin Babiker A. Mustafa[2], Ismail El-Azhary[3]
[1, 2] Dept. of Telecommunications, Faculty of Engineering, Al Neelain University, Khartoum, Sudan
[3] Dept. of Computer Engineering, Faculty of Engineering, Al Neelain University, Khartoum, Sudan

Abstract: ***Worldwide Interoperability For Microwave Access Technology (WiMAX), broadband wireless communications cosidered as one of the most growing and developing technology in the field of telecommunications[1] . Mobile multi-hop relay (MMR) Worldwide Interoperability for Microwave Access (WiMAX) networks uses Relay stations (RSs) to extend the cell coverage and enhances the link quality and the throughput . In MMR WIMAX networks, the number of hopes between the subscriber Stations (SSs) and the Base Station (BS) is allowed to be more than two hops when Non Transparent RS (NT-RS) is used [2]. Wireless networks are inherently less secure compared to their wired counterparts due to the lack of physical infrastructure. In this paper the Self Organized Efficient and Authentication Key management protocol (SEAK) were modified, the proposed protocol introduces different service levels according to user needs .***

Keyword: MMR, PDU, SEAK

I. INTRODUCTION

The Self Organized Efficient and Authentication Key management protocol (SEAK), is one of Mobile Multi-hope Relay (MMR) WIMAX security protocol. In the proposed protocol which is based on (SEAK) protocol, classification and improvement will be discussed, three classes will be introduced A, B and C.

Cost of each class calculated in terms of bytes, each class could be used according to user needs.

II. METHODOLOGY

The communication cost of MMR WiMAX consists of two parts, the cost of authentication and key management to update table and the cost of group key update commands messages for secure communication. These updating is directly proportional to the number of hops, number of bytes and the total number of messages transmitted. For calculating the communication cost of overall MMR WiMAX networks, equation 2.1 is used.

$$C = h \sum_{A=1}^{k} (S_A) \qquad 2.1$$

Where
C = Total communication cost
h = Hop count
K = Total number of message
S*k* = Size of bytes, where k is the integer from 1-k

2.1.1 Class A (single hope)

In this class ,the number of Authentication message are four (information ,request ,response and acknowledgement) length of messages were assumed according to reference[1] . equation 2.2 is used for calculating total cost for class A single hope

$$C = \sum_{A=1}^{4} (S_{PKM}) + \sum_{A=1}^{k=2} (S_{AK}) + \sum_{A=1}^{k=2} (S_{TEK}) + \sum_{A=1}^{k=2} (S_{RA}) * P \qquad 2.2$$

C = 18+2+2+2*p
C = 22+2p
Where P is the probability of reauthentication.

2.1.2 Class A (multi hope

In this situation packet data unit (PDU) is used to carry all message of the propsed protocol , PDU parts lengths were assumed according to reference [1], equation 2.3 is used for calculating total cost for class A multi hope.

$$C = \sum_{A=1}^{k=2} (S_{PKM}) + \sum_{A=1}^{k=2} (S_{AK}) + \sum_{A=1}^{k=2} (S_{TEK}) + \sum_{A=1}^{k=2} (S_{RA}) * P \qquad 2.3$$

Cn = 2(n+16)(p+3)
Where n is the hop number

2.2.1 Class B (single hop)

In this class the number of Authentication message are three (request , respone and acknowledgment). Lengths of messages were assumed according to reference[1]. Equation 2.4 is used for calculating total cost for class B single hop.

$$C = \sum_{A=1}^{3}(S_{PKM}) + \sum_{A=1}^{k=2}(S_{AK}) + \sum_{A=1}^{k=2}(S_{TEK}) + \sum_{A=1}^{k=2}(S_{RA}) * P \qquad 2.4$$

C=21+2P

2.2.2 Class B (multihop)

In this situation packet data unit (PDU) is used to carry all messages of the proposed protocol, PDU parts lengths were assumed according to reference[1]. Equation 2.5 is used for calculating total cost for class B multi hop.

$$C = 2h\sum_{A=1}^{k=2}(S_{PKM}) + 2h\sum_{A=1}^{k=2}(S_{AK}) + 2h\sum_{A=1}^{k=2}(S_{TEK}) + 2h\sum_{A=1}^{k=2}(S_{RA}) * P \qquad 2.5$$

=32+32+32+32*P=96+32P

2.3.1 Class C (single hop)

The number of authentication message in this class are tow (request and respone). Lengths of message were assumed according to reference[1]. Equation 2.6 is used for calculating total cost for class C single hop.

$$C = \sum_{A=1}^{k=2}(S_{AUTH}) + \sum_{A=1}^{k=2}(S_{AKREF}) + \sum_{A=1}^{k=2}(S_{TEKRA}) + \sum_{A=1}^{k=2}(S_{RA}) * P \qquad 2.6$$

=14+2+2+2P
= 18+2P

2.3.2 Class C (multihop)

All messages of the proposed protocol were carried through (PDU), PDU parts lengths were assumed according to reference[1]. Equation 2.7 is used for calculating total cost for class C multi hop.

$$C = \sum_{A=1}^{K=2}(S_{pkm}) + \sum_{A=1}^{k=2}(S_{AKREF}) + \sum_{A=1}^{k=2}(S_{TEK}) + 2h\sum_{A=1}^{k=2}(S_{RA}) * P \qquad 2.7$$

=(15+15) + 30 +30 +30P
=90+30P=30(3+p)

2.4.1 SEAK(single hop)

The number of authentication messages are three (information , request and response) The cost of seak (single hope) is 15+2+2+2P = 19+2P [1].

2.4.2 SEAK (Multi hop)

Seak for multihop PDU message payload = 13 byte
The total length of pdu =13 + 4 (header) =17
C_n =2 (15 +n) (3+P) [1]

III. RESULTS AND DISCUSSION

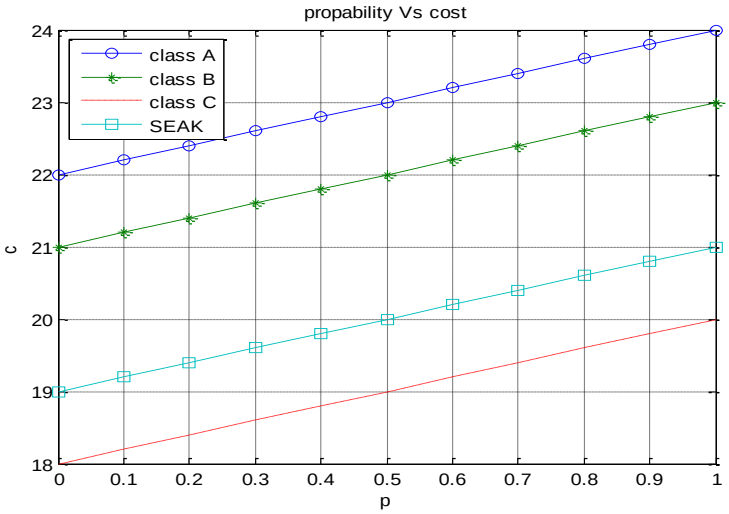

Fig 3.1

Fig3.1 above explain the total cost of all classes A , B , C and SEAK protocol versus propbility of failure in single hop mode. It is clear that the cost increases with the propbility increasing in linear manner, for all classes and seak protocol the rate of increasing is 0.2 byte for every propbility unit (0.1

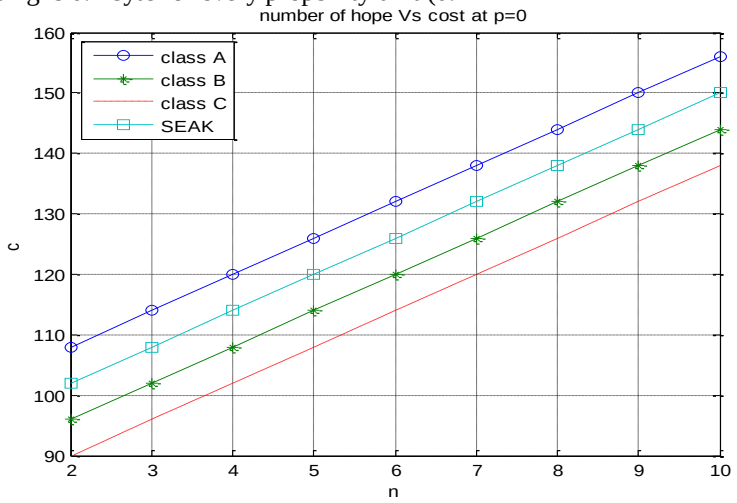

Fig3.2

Fig3.2 above shows the tota costl of classes A ,B , C and SEAK versus number of hops for propbility of failare p=0 (network without failure).The total cost of all classes and seak protocol increases linearly with number of hops. The rate of increment is 6 bytes per hop.

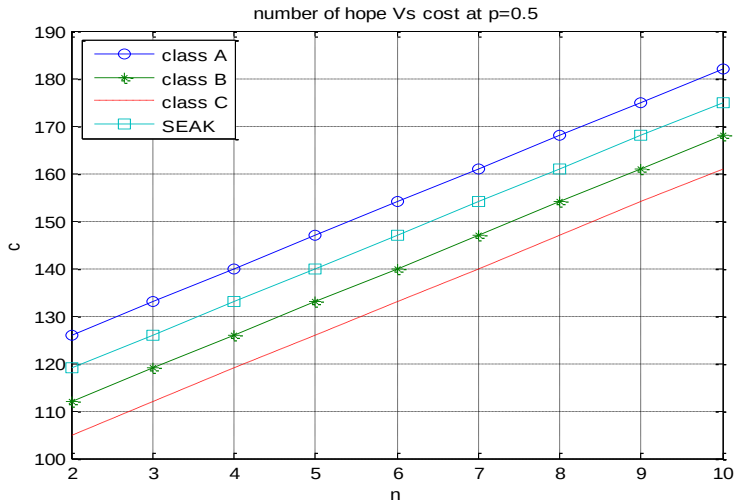

Fig3.3

Fig3.3 above illustrates the total cost of classes A , B , C and SEAK versus number of hops, for every hop the increasing of total cost for all classes A , B ,C AND seak is 7 bytes.

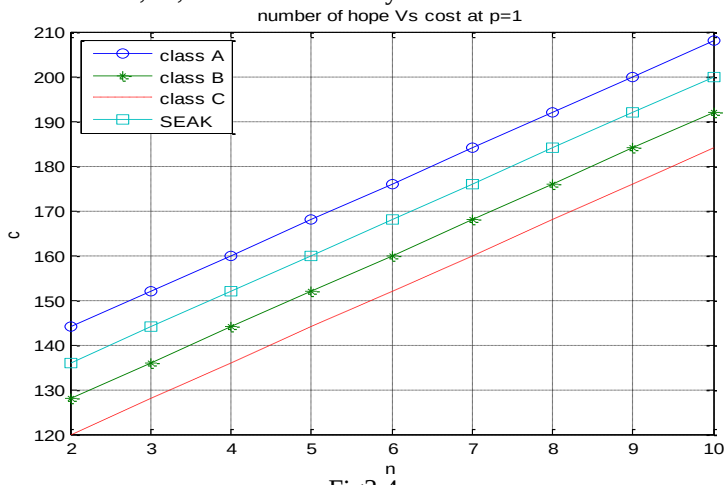

Fig3.4

Fig3.4 shows the total cost of classes A , B , C and SEAK versus number of hops for p=1 (maximum propbility), it is clear that the rate of total cost increasing is 8 bytes for each hop.

IV. CONCLUSION

- In single mode class C has less total cost than the total cost of SEAK, where classes A & B has total cost higher than SEAK.
- In multihop at p = 0, 0.5 and (1), classes B and C have less total cost than the SEAK.
- Class A in single mode and multimode for every probability of failure has maximum total cost.
- In multihop the rate of total cost increment increases with the probability of failure increasing which indicate that the probability of failure has significant effect to total cost. .
- whatever most challenges of wimax networkes exist in multihop, e.g probability of failure (denial of sevices), e.t which necessitates using the proposed protocol for minimizing total cost and introducing different classes according to user needs .

REFERENCES

[1] Adnan Shahid Khan, Medium Access Control Security Mechanism for Mobile Multi-hop Relay WiMAX networks, May 2012.

[2] F .E. Ismael , S. K. Syed-Yusof, M. Abbas, N. Fisal and N. Muazzah, Frame structure for Mobile Multi-hop relay (MMR) WiMAX networks, International Journal of Physical Sciences,May 2013.

ABOUT AUTHOR

Salih Yasien Salih has a B. Sc. in Communication Engineering from the University of Alexandria (1987) and an M. Sc. in Computer Engineering and Networks from Algazeera University (2002).Salih is now doing his PhD research in the field of QoS with the Department of Telecommunications, Al Neelain University. He worked as a manager of CCS Company for Computer and Networks for two years . He is also worked as a lecturer at the Army Institution for Information Systems for three years. He used to be a technical advisor for the Armed Forces for five years. He is working as a lecturer in many Sudanese universities and institutions. His research interest includes quality and services, and its application to the communication field

Amin Babiker A/Nabi Mustafa obtained his B.Sc. & M.Sc. from the university of Khartoum in 1990 & 2001 respectively. He obtained his Ph.D. from Alneelain University in 2007. He was the head of Computer Eng. Dept. from 2001 to 2004. Then he became the vice-dean. He has been the dean, Faculty of Engineering Alneelain University since 2009. His research areas include QoS in Communication Systems, Traffic Engineering, Service Costing Disciplines & Networking. Associate Prof. Dr. Amin is a Consultant Engineer. He is a member of the Sudan Engineering Council. He is also a member of the Executive Committee of the Federation of Sudanese Engineers. Dr. Amin supervised or supervising more than 40 Ph.D. or M.Sc. students.

Ismail El-Azhary received his BSc (Hons) degree from the University of Khartoum (Sudan) in1979. In 1989 he obtained his PhD degree from the University of Bradford (UK). He joined Omdurman Islamic University in 1992 as an assistant professor. Then, he moved to the Sudan University of Science and Technology as an associate professor in 1994. He became the Dean of the Faculty of Engineering, Al Neelain University from 2000 to 2005. His research interests include: QoS of networks, technical communication, digital typography, e-learning, antennas and propagation, and embedded systems. Professor El- Azhary is a Chartered Engineer and member of the IET.

