ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 12, December 2014

Hop By Hop Authentication for Source Intermediate Node Privacy Protection in Wireless Sensor Network

M.Saravana Muthu Pandian[1], S.S.Jaya[2], K.Mohan Kumar[3]

P.G. Scholar, Department of CSE, R.V.S. College of Engineering and Technology, Coimbatore, India[1].

Assistant Professor, Department of CSE, R.V.S. College of Engineering and Technology, Coimbatore, India[2].

P.G. Scholar, Department of EST, Easwari College of Engineering, Chennai, India[3].

ABSTRACT: The Internet Key-Exchange (IKE) protocols are the core cryptographic protocols to ensure Internet security, which specify key exchange mechanisms used to establish shared keys for use in the Internet Protocol Security (IPsec) standards. For key-exchange over the Internet, both security and privacy are desired. For this reason, many message authentication schemes have been established, created on both symmetric-key cryptosystems and public-key cryptosystems. But it has the limitations of high computational and communication overhead in addition to lack of scalability and resilience to node compromise spells. The proposed scheme is Signature and ID generation, which are used to provide high security to message passing in Internet. This proposed method is an efficient key management framework to ensure isolation of the compromised nodes. Each node will have individual signature, and each message passing between intermediate nodes have one key to authenticate. Message passing between each nodes have an authentication using signature and key. This effective method will give high secure to message passing other than existing methods in Internet.

KEYWORDS: Elliptic curve cryptograph; deliver ratio; Message delay; UBUNTU; Energy consumption

I. Introduction

Key-exchange (KE) is a traditional zone of cryptography. Nevertheless, key-exchange is also a quite superior area of cryptography, in opinion of its seemingly humble yet inaccuracy prone landscape. Explicitly, most key-exchange protocols appear to be very modest and even innate, and thus seeming to be simply designable, but the literature has been witnessing that the design of correct and secure KE turns out to be extremely error prone and could be notoriously subtle and difficult (the literature is filled with protocols that have been found to contain certain security flaws).User authentication limits the legitimacy of the envisioned parties in real time. For example, in a Client - server request, a service benefactor desires to confirm the legality of a user before if services to the user. Likewise, a user needs to make sure that the service provider is unaffected so that the user is keen to send its sensitive information (such as a credit card number) to the service provider. Later communicating parties need a communal key to encrypt and decrypt data; shared-key validation makes certain that the shared communal key is identified only to the anticipated parties. In a key-agreement protocol without user validation, an invader can misrepresent the uniqueness of a blameless party, foremost to spells such as replay, resource exhaustion and indefinite key share.

Deniability is a privacy property that ensures protocol participants can later deny pleasing part in a exact protocol run. Such a property has been affirmed as necessary for new protocols offered to secure the IP (Internet Protocol) level on Internet communications. Traditional deniability only deliberates the privacy of the honest verified against a perhaps malicious verifier, and involves that the interactions between them be computationally simulatable, i.e., computational zero-knowledge (ZK). A tougher form of deniability can be accomplished by collective key authentication. With a shared key resolution, whichever user in the protocol run could have shaped all the messages in the run. A uniform tougher form of deniability can be accomplished when the shared key is gotten using techniques from identity-based cryptography. One of the simple secure communication technologies is the key establishment protocol that is identified

10.15680/ijircce.2014.0212061

as Internet Key Exchange (IKE). It is the typical of Internet protocol Security (IPsec) offered by the IETF in 1998. In computing, Internet Key Altercation (IKE or IKEv2) is the protocol used to set up a security association (SA) in the IPsec protocol group. IKE shapes upon the Oakley protocol and ISAKMP. IKE imposts X.509 certificates for authentication - both pre-shared or distributed by DNS (preferably with DNSSEC) and a Diffie–Hellman key exchange - to set up a collective session furtive from which cryptographic keys are imitative. In addition, a security policy for each peer which will link must be manually conserved.

Most IPsec executions consist of an IKE daemon that runs in user space and an IPsec stack in the kernel that processes the actual IP packets. User-space daemons have easy contact to mass storage encompassing configuration information, such as the IPsec endpoint discourses, keys and certificates, as indispensible. Kernel segments, on the other hand, can progression packets adeptly and with lowest overhead—which is energetic for performance motives. The IKE protocol customs UDP packets, typically on port 500, and mostly entails 4-6 packets with 2-3 turn-around times to make an SA on together sides. The exchanged key substantial is then specified to the IPsec stack. For occasion, this could be AES key material identifying the IP endpoints and ports that are to be susceptible, as well as what kind of IP Sec tunnel has been designed. The IPsec heap, in turn, diverts the relevant IP packets if and where proper and realizes encryption/decryption as mandatory. Enactments vary on how the capture of the packets is finished—for example, explicit use virtual devices; others yield a cut out of the firewall as well.

II. Related work

Traditional deniability only considers the privacy of the honest prover beside a probably malicious verifier, and necessities that the interfaces between them be computationally simulatable, i.e., computational zero-knowledge (ZK).That is, given a session transcript, the malicious verifier cannot prove that the honest prover was ever involved in the conversation. However, as clarified by Di Raimondo, there are scenarios in which deniability is actually a concern to the receiver's privacy as well. What we would like to happen is that if the prover acts honestly during the protocol, it also should not be able at a later stage to claim the messages are authentic in order to violate the privacy of the verifier. This property is called forward deniability, asithas some affinity to the notion of forward secrecy. It is shown that computational ZK does not guarantee forward deniability, but statistical ZK does.

The security of DIKE is analysed in unity with the Canetti-Krawczyk context (CK-framework) with post-specified nobles in the random oracle (RO) model. We also make negotiations on a list of concrete yet indispensible security possessions of DIKE, most of which are outside the CK-framework. We then describe CNMSZK for DHKE, beside with complete elucidations and explanations. To our knowledge, our creation of CNMSZK for DHKE approaches for the toughest definition of deniability, to date, for key-exchange etiquettes. The CNMSZK property of our protocols is analysed in the limited random oracle model, under an allowance of the knowledge-of-exponent statement named coexisting knowledge-of-exponent (CKEA) that might be of liberated interest.

III. Proposed algorithm

In this project, a secure and efficient source unspecified message authentication method is planned with active algorithm Elliptic Curve Cryptography (ECC). This arrangement is secure against adaptive chosen-message spells. This scheme enables the transitional nodes to authenticate the message so that all corrupted message can be perceived and dropped to protect the sensor power. While achieving conciliation resiliency, flexible-time validation and source individuality protection, our scheme does not have the threshold delinquent. It progresses a source unidentified message authentication code on elliptic curves that can afford absolute source anonymity. It compromises an effective hop-by-hop message authentication mechanism for WSNs without the threshold restriction. It devises network execution criteria on source node privacy protection in WSNs. It suggests an efficient key management framework to guarantee isolation of the negotiated nodes. To the best of our knowledge, this is the first scheme that affords hop-by-hop node authentication without the threshold restraint, and has concert better than the symmetric-key based schemes. The distributed landscape of our algorithm makes the pattern fit for decentralized networks.

10.15680/ijircce.2014.0212061

A. *Introduction to UBUNTU:*

Ubuntu is a Debian-based Linux functional system, with Unity as its defaulting desktop location. It is founded on free software and named after the Southern African philosophy of Ubuntu (literally, "human-less"), which frequently is translated as "humanity towards others" or "the belief in a collective bond of provision that links all humanity". Convening to particular metrics, Ubuntu is the extreme popular Linux dispersion.

B. *Network Topology:*

The Physical Coating is the first and lowest deposit in the seven-layer OSI model of computer networking. The execution of this layer is regularly categorized PHY. The Physical Layer consists of the simple hardware transmission tools of a network. It is a vital layer underlying the logical data structures of the developed level functions in a network. Due to the plethora of offered hardware technologies with usually varying characteristics, this is perhaps the utmost complex level in the OSI architecture.

C. *TCL language:*

The Physical Layer describes the means of transmitting raw bits rather than reasonable data packets over a physical association connecting networking nodes. The bit stream may be assembled into code words or symbols and renewed to a physical that is transmitted over hardware**.** It is frequently used for hurried prototyping, scripted applications, GUIs and analysis. TCL is used on embedded tight platforms, together in its full custom and in other small-footprint sorts.

IV. SOFTWARE DESCRIPTION

A. *Network Simulator-2:*

In 1996-97, ns version 2 (ns-2) was commenced based on a refactoring by Steve McCanne. Usage of Tcl was replaced by MIT's Object Tcl (OTcl), an object-oriented parlance of Tcl. The core of ns-2 is also transcribed in C++, but the C++ simulation objects are related to shadow objects in OTcl and variables can be allied between both linguistic realms. Simulation scripts are inscribed in the OTcl language, an allowance of the Tcl scripting language. Currently, ns-2 entails of over 300,000 lines of foundation code, and nearby is possibly an equivalent amount of subsidised code that is not integrated directly into the main distribution (numerous splits of ns-2 occur, together preserved and unmaintained). Moreover it scores on GNU/Linux, Free BSD, Solaris, Mac OS X and Windows 95/98/NT/2000/XP as well. It is permitted for use below version 2 of the GNU General Community Authorization.

B. *TCL language:*

TCL-Tool Command Language is a scripting language formed by “John Ousterhout”. It is generally used for express prototyping, scripted solicitations, GUIs and testing. TCL is used on embedded structures platforms, both in its full method and in numerous other small-footprint varieties. However the execution to the writer, through programmers sprouting their own idioms estimated to be embedded into submissions, TCL gained reception on its private.

C. *Node formation:*

This segment is formation of nodes what all desirable for transfer and receiving information. One node is supposed as sender node and another node is expected as receiver node. And some nodes are implicit as information passing nodes. In communication networks a node is whichever a connection point a restructuring point or a message end point. It is used for connection-oriented transmissions; however the connectionless consumer datagram suite (UDP) is used for simpler messaging transmissions. TCP is the further complex protocol, due to its stateful proposal incorporating consistent transmission and data stream amenities. The utmost well-known transport protocol is the (TCP). It hired its name to the title of the perfect internet protocol suite TCP/IP.

V. RESULT AND DISCUSSION

We instrument the bivariate polynomial established scheme and our suggested scheme in a real biosphere Valuation. The appraisal is based on similar security levels. The bivariate polynomial-based scheme is a symmetric key based execution, while our pattern is established on ECC.

10.15680/ijircce.2014.0212061

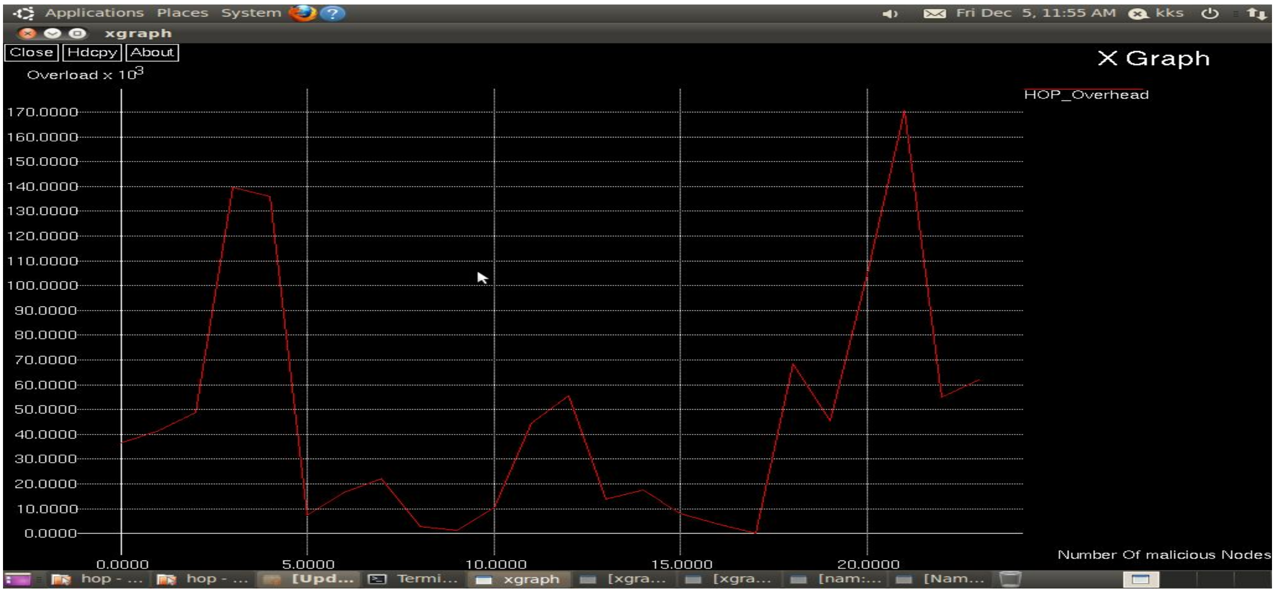


Fig.1. Message Delay

The simulation results in Fig.1 and Fig.2 demonstrate that our proposed scheme has a greatly lower energy consumption and message transmission delay.

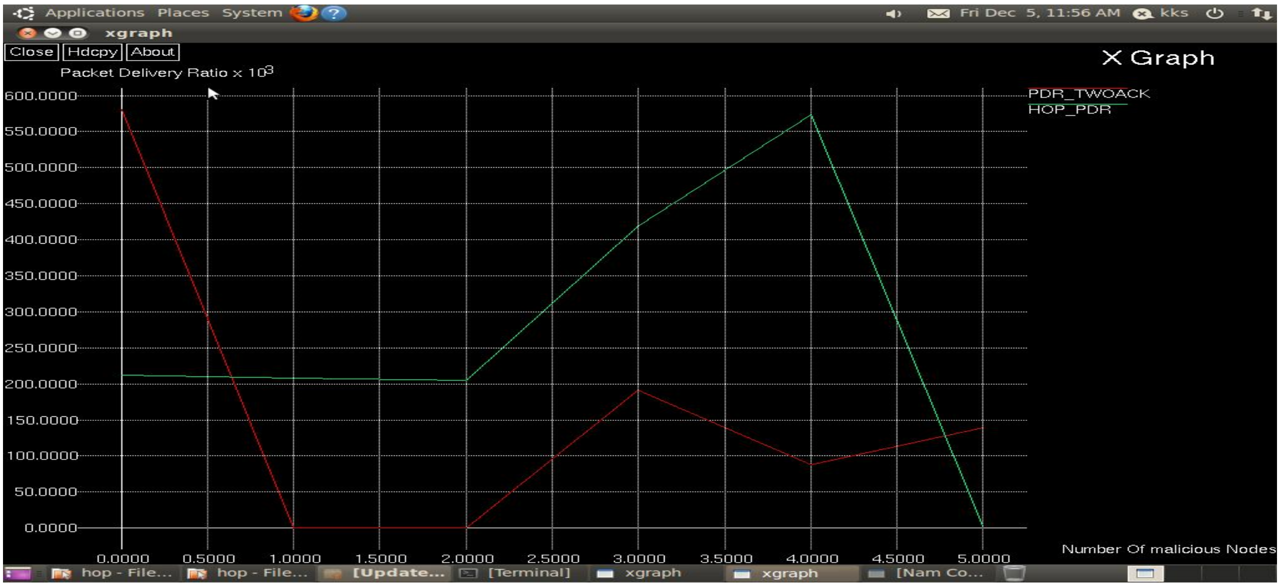


Fig.2. Delivery Ratio

The great communication upstairs of the polynomial recognized scheme will increase the energy consumption and message delay.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 12, December 2014

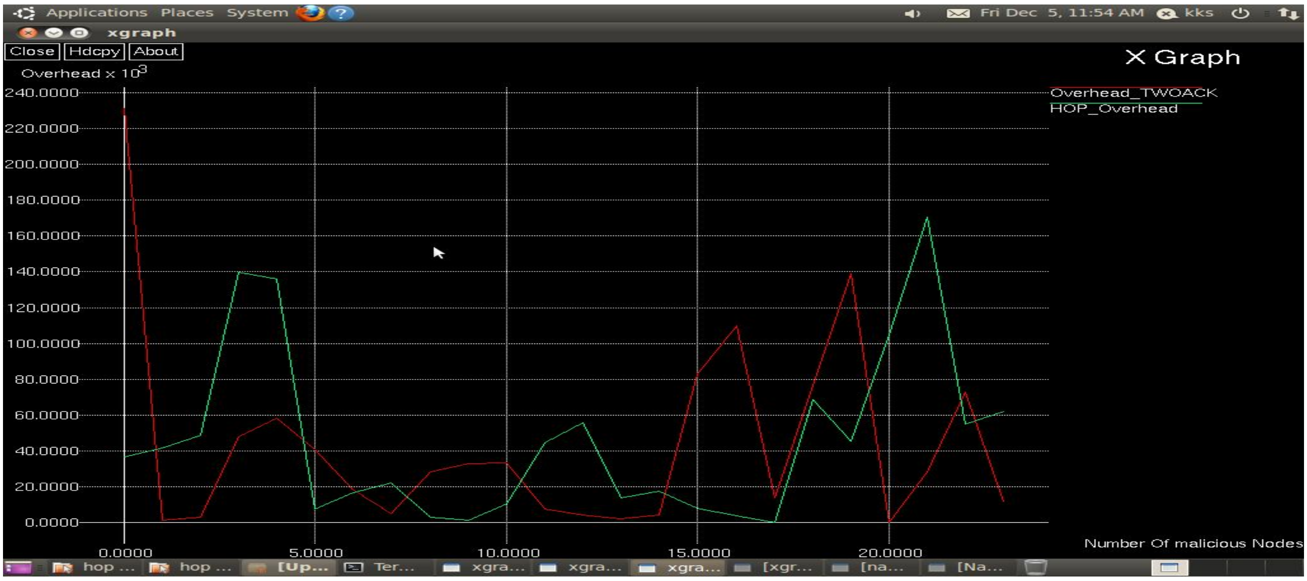
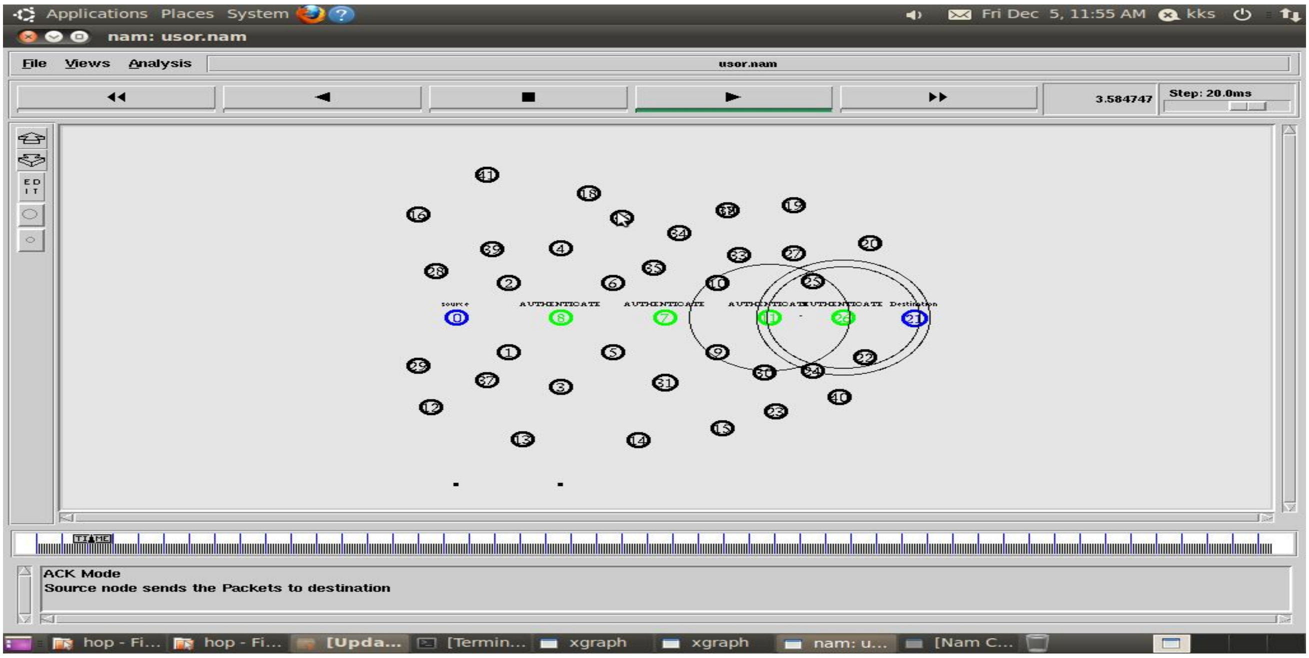


Fig.3. Energy Consumption

The simulation results in Fig.3 and Fig.4 demonstrate that our proposed scheme has plentiful lower energy consumption and message source node sends the packets to endpoint.



ACK Mode
Source node sends the Packets to destination

Fig.4. Source Node Sends the Packets to Destination

The simulation results in Fig.5 and Fig.6 demonstrate that our offered scheme Source Selects the Substitute Path to Transmit the Data to Mr Report to Destination and Destination Node Authenticates the Misbehaviour Report.

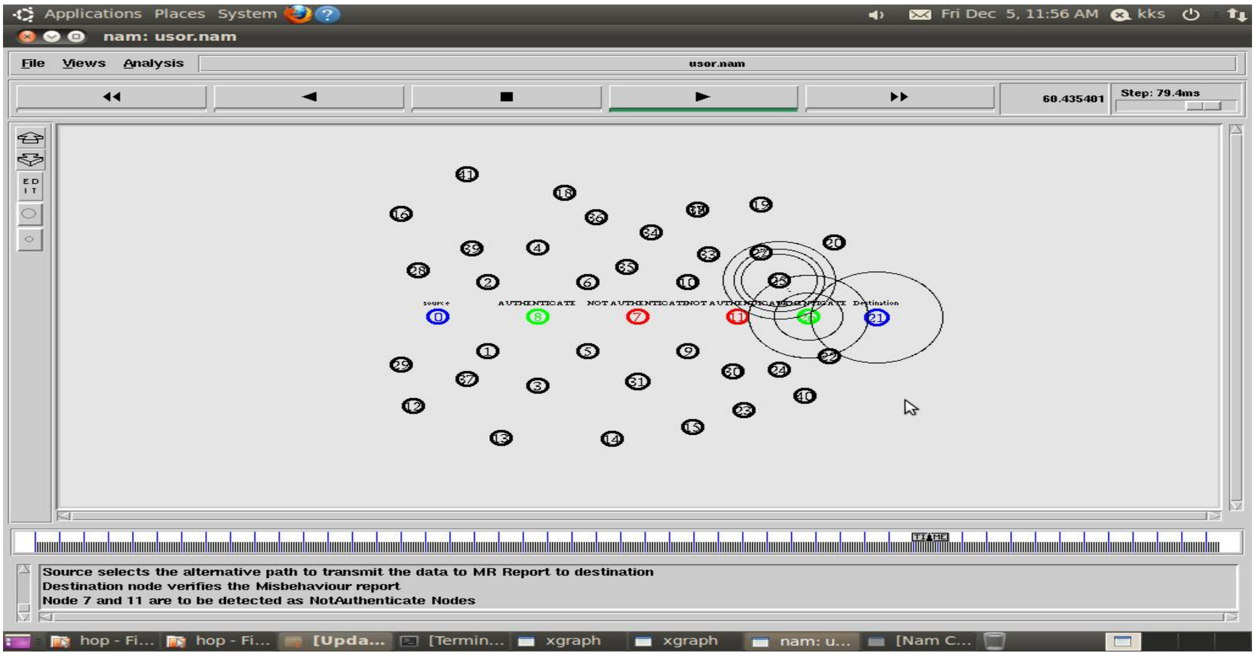
10.15680/ijircce.2014.0212061

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

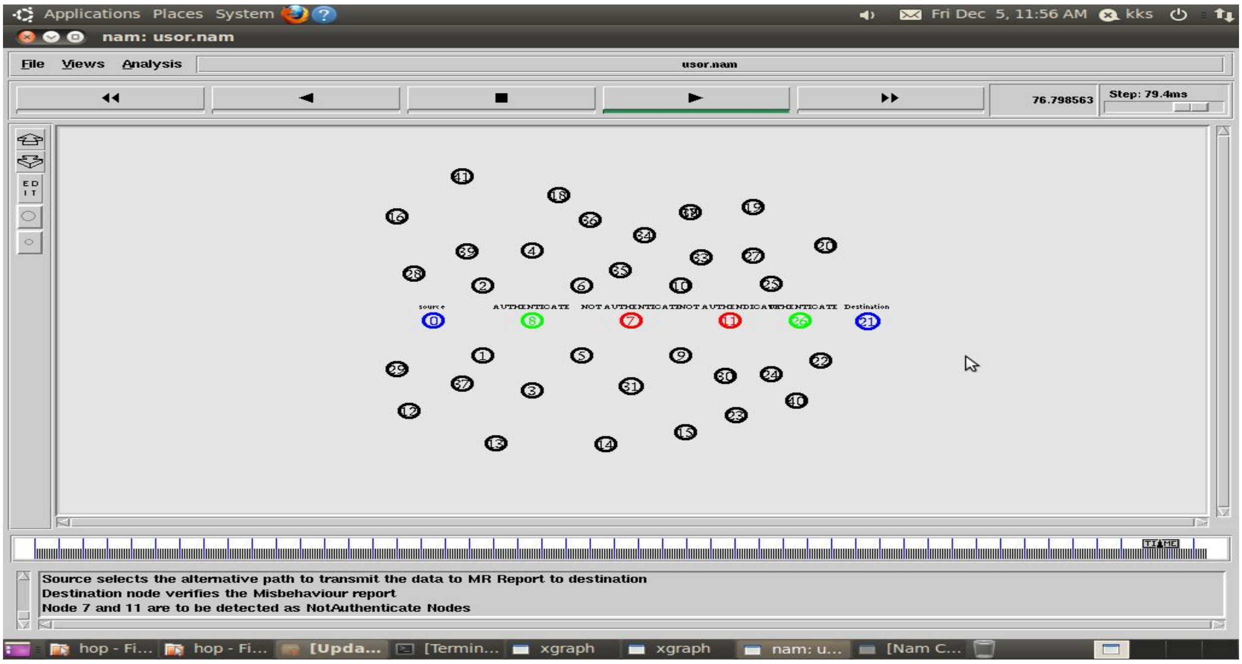
(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 12, December 2014



Source selects the alternative path to transmit the data to MR Report to destination
Destination node verifies the Misbehaviour report
Node 7 and 11 are to be detected as NotAuthenticate Nodes

Fig.5. Source Selects the Alternative Path to Transmit the Data To Mr Report to Destination



Source selects the alternative path to transmit the data to MR Report to destination
Destination node verifies the Misbehaviour report
Node 7 and 11 are to be detected as NotAuthenticate Nodes

Fig.6. Destination Node Verifies the Misbehaviour Report

VI. CONCLUSION AND FUTURE WORK

Here the established information is the suggested proficient source intermediate node message authentication scheme based on signature and ID generation afford high security than the other methods in the surviving research. The

10.15680/ijircce.2014.0212061

excluding results is, our proposed scheme is more proficient than the bivariate polynomial-based scheme in terms of computational overhead, energy feasting, distribution ratio, dispatch delay, and memory feeding. Although confirming message sender privacy, this system can be realistic to any message to provide message content legitimacy. To deliver hop-by-hop message authentication without the weakness of the built in threshold of the polynomial-based scheme, we then suggested a hop-by-hop message authentication scheme based on the Signature and ID generation.

REFERENCES

1. Perrig, R. Canetti, J. Tygar, and D. Song, "Efficient Authentication and Signing of Multicast Streams over Lossy Channels,"Proc. IEEE Symp. Security and Privacy May 2000.
2. Blundo, A. De Santis, A. Herzberg, S. Kutten, U. Viceroy, and M. Yung, "Perfectly-Secure Key Distribution for Dynamic Conferences,"Proc. Advances in Cryptology (Crypto '92), pp. 471-486, Apr.1992.
3. H. Wang, S. Sheng, C. Tan, and Q. Li, "Comparing Symmetric-Key and Public-Key Based Security Schemes in Sensor Networks: A Case Study of User Access Control,"Proc. IEEE 28th Int'l Conf. Distributed Computing Systems (ICDCS), pp. 11-18, 2008.
4. K. Nyberg and R.A. Rueppel, "Message Recovery for Signature Schemes Based on the Discrete Logarithm Problem,"Proc. Advances in Cryptology (EUROCRYPT), vol. 950, pp. 182-193, 1995.
5. T.A. ElGamal, "A Public-Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms,"IEEE Trans. Information Theory, vol. IT-31, no. 4, pp. 469-472, July 1985.
6. M. Albrecht, C. Gentry, S. Halevi, and J. Katz, "Attacking Cryptographic Schemes Based on 'Perturbation Polynomials'," Report 2009/098, http://eprint.iacr.org/, 2009.
7. W. Zhang, N. Subramanian, and G. Wang, "Lightweight and Compromise-Resilient Message Authentication in Sensor Networks,"Proc. IEEE INFOCOM, Apr. 2008.

BIOGRAPHY

Mr.M.Saravana muthu pandian Pursuing Master of Engineering in Computer Science Engineering in R.V.S. College of Engineering and Technology, Coimbatore, India. He received his Bachelor Degree in Jaya Engineering College, Chennai. His area of interest in computer networks, Image processing, cloud computing.

Mrs.S.S.Jaya currently working in R.V.S. College of Engineering and Technology as Assistant Professor, Department of computer science engineering, Coimbatore, India. Her area of interest in cloud computing, Image processing, Data structures, computer networks.

Mr.K.Mohankumar Pursuing Master of Engineering in Embedded System Technologies in Eswari College of Engineering , Chennai, India. His area of interest in Cloud computing embedded control systems, networks.

,

10.15680/ijircce.2014.0212061