International Journal of Engineering & Technology, 7 (2.26) (2018) 35-39

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research paper

A survery on platform of secured routing algorithm

Miss. Divya [1] , Dr. R. Gobinath [2]

[1] Research Scholar, Department of Computer Science, Vels Institute of Science, Technology and Advanced Studies (VISTAS), Pallavaram, Chennai, Assistant Professor, Department of Computer Science, Prince Shri Venkateshwara Arts and Science College – Chennai.
[2] Assistant Professor, Department of Computer Science, VISTAS, Pallavaram, Chennai.
**Corresponding author E-mail: iamgobinathmca@gmail.com*

Abstract

This paper describes the characteristics and techniques of Ad Hoc network. Ad Hoc networks are temporary network, set anywhere without any need of external infrastructure like wires. The essential premise of this paper is to exchange confidential message over wireless medium without route break and unauthorized eavesdroppers. In recent years, the research of routing protocol for AdHoc network has caused public concern widely. The multi hopping routing protocol has failed to meet the needs of network topology and route restructure. It must also consider the bandwidth and high error rate. The new routing protocol suitable for solving these problems in Ad Hoc network is AODV.

Keywords: *Ad Hoc Network; Network Security; Routing; AODV Routing Protocol*

1. Introduction

A computer network is a gathering of computer systems and other computing hardware resources that are allied together through communication channels to promote transmission and resource-sharing amid a broad area of users. Networks are frequently assorted based on their aspects. Computer networks support a vast number of relevance and services such as approach to the World Wide Web, digital video, digital audio, shared use of application and storage servers, printers, and fax machines, and use of email and instant messaging applications as well as many others. Computer networks vary in the communication medium used to transfer their signals, communications protocols to formulate network jam, the network's size, topology and organizational intent. The prime familiar computer network is the Internet.Computer communication junction carries data as a bit flood. However, maximum messages in computer networks are toted in packets. A network packet is a patterned unit of data (a list of bits or bytes, usually a few tens of bytes to a few kilobytes long) transmitted by a packet-switched network. In packet networks, the data is patterned into packets that are directed through the network to their target. Once the packets reach they are gathered into their initial message. In communication networks, a node is either a redistribution point or a communication endpoint. A physical network node is an operative computerized device that is connected to a network, and is efficient of creating, receiving, or transmitting messages over a transmission channel. In telecommunications, data transfer between the node-to-node is the flow of data from one node of a network to the next. In the OSI model it is managed by the least two layers, the data link layer and the physical layer. Routing determines good passage through a network to carry the message from source to target. Routing is the manner of choosing network paths to carry network jam.

2. Review of literature

An implementation study of AODV routing protocol [6] express the evolution in AODV protocol. The AODV is implemented in Linux Kernel because of its implicit portability and wide source nature of Linux. AODV protocol manages an orbital timer for updating multicast route table access. Security Enhancements in AODV protocol for wireless Ad hoc networks [7] withstands certain misbehavior provoked by malign node for AODV routing protocol. This paper proposes the security schemes to prevent the internal attacks. An Intrusion Detection and Intrusion Prevention method is also discussed to prevent several attacks in network.
AODV with Path Accumulation [8] examines the expected alterations by organizing the path accumulation feature in AODV. The texture of protocol helps to minimize the routing capacity and sustain excellent performance. This paper introduces the advanced protocol AODV-PA to enhance the performance. The AODV-PA (path accumulation) aids to minimize the number of route discoveries than AODV. Multi – linked AODV Routing protocol for wireless Mesh network [9] symbolizes the modified AODV protocol called AODV-ML (multi link). This protocol successfully observes the bidirectional channel between neighboring nodes in multi hop wireless network. This work achieves high stable of efficiency by acquiring reduced overhead. High performance AODV routing protocol for Hybrid wireless Mesh Network [10] instants an advanced protocol called AODV-HP (hybrid protocol) which is derived from AODV protocol. This protocol ease the issue associated with the physical, MAC and network layer in hybrid WMNs. Combat with Black Hole attack in AODV routing protocol in MANET [11] demonstrates MAODV schema which is used to combat black hole attack in AODV routing protocol. This paper also reviews the security problem of MANET. Global Mobile Simulator is used to gain the prescribed security with limited delay and overhead.

Copyright © 2018 Miss. Divya, Dr. R.Gobinath. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Bypass AODV: Improving Performance of Ad hoc On-demand Distance Vector (AODV) routing protocol in wireless Ad hoc Networks [12] enumerates that Bypass-AODV is derived to enhance the utilization of AODV routing protocol. Bypass-AODV adopts an explicit strategy of cross-layer MAC-interaction to establish mobility-related route breaks. This paper also illustrates the encounter on node density and portability of Bypass-AODV.A dynamic Anomaly Detection scheme for AODV – Based mobile Ad hoc networks [13] reports a new dynamic anomaly detection technique for MANET. For elevating the security robust learning techniques are used. Misuse detection and Anomaly detection techniques are recycled for identifying malicious attacks. In Anomaly detection method the packet carried at each node is inspected.

Performance evaluation of energy consumption for AODV and DSR routing protocols in MANET [14] inspect the valuation of energy consumption of AODV routing protocol. The operation of this research comprises simulation scenario, portability arrangement and energy arrangement. AODV protocol endures route discovery and route maintenance to manage routing information. An Energy efficient routing protocol decreases the power consumption of the nodes. Research of AODV routing protocol for Ad hoc networks [15] characterize the basic properties of Ad hoc network. An AODV protocol represents an optimized protocol called B-AODV established on shortage of route finding and routing reformation on AODV. This paper also abstracts the performance of routing protocol build upon routing overhead, node delay, packet success rate and so on. The prime protocol upgrades the route reformation capacity and minimizes the routing overhead. The above table describes the list of measurements taken in secured Ad HOC networks. These works specifies the list of methods and tech-niques used to transfer the data securely in the wireless network environment. The table also mentions how different Authors used various security algorithms to solve the network security issues. The above table discusses various applications of AODV routing protocol and also describes how various authors used this protocol to solve the problem of route break in network routing while transmitting the valuable data over secured wireless network. The TABLE II also explains about various measurements observed by different authors in AODV routing protocol with network security.

3. Existing work

Table 1: Measurements Taken in Network Security

SNO	YEAR	AUTHOR	TOPIC	MEASUREMENS	DESCRIPTION
1	DEC 1999	Lidong Zhou , Et al.	Securing Ad hoc Networks	Threshold Secrecy	This paper studies about the network security issues using multiple routing techniques in cryptography.
2	MAR 2000	Piyush Gupta, Et al.	The capacity of wireless networks	Throughput & Capacity	This paper investigates the network security level in ALOHA network using TDMA, FDMA & CDMA.
3	2005	Michael J. Neely, Et al.	Capacity and Delay Trade-offs for Ad Hoc Networks	Capacity & Delay	This paper describes the problem of security in cell partitioning network using two hop relay
4	2005	Patrick Herhold, et al.	Cooperative Multi hop Transmission in wireless network	Capacity	This paper studies the issues of network security in two hop algorithm and provides secured data transmission using multi hopping.
5	SEP 2007	ShabnamShafiee, et al.	Secrecy Capacity of Gaussian MIMO Wire-tap channel	Secrecy capacity, Secrecy rate & Power Allocation	This paper investigates secured data communication in MIMO wiretap channel using multiple antenna system in cryptographic methods.
6	2008	F. Oggier, et al.	The MIMO Wiretap Channel	Equivocation rate, secrecy rate & Secrecy capacity	This paper describes the issues in single antenna system and provides solution using multiple antenna channels in Information Theoretic System.
7	OCT 2008	OnurOzanKoylough, et al.	Interference Alignment for Secrecy	Equivocation rate, Secrecy rate & Secrecy capacity	This paper explains the secured data transmission using wiretap channels in Information Theoretic System.
8	MAR 2010	S. Anand, R.Chandra-mouli (IEEE Members)	On the Location of an Eavesdroppers in multi terminal networks	Secrecy capacity, Power allocation	This paper studies about network security issues in cryptographic methods using artificial noise generation in Information Theoretic System
9	JUN 2010	Xiangyunzhou et al.	Secure Transmission with Artificial Noise over Fading Channels	Capacity, Power Allocation	This paper investigates the network security problem during data transmission using cryptographic methods.
10	JUN 2010	AshishKhisti, Et al.	Secure Transmission with the MIMOME Wiretap Channel	Secrecy capacity, Throughput	This paper describes the issues in secured data transmission using multiple antenna system
11	FEB 2011	Pedro C. Pinto, et al.	Wireless Secrecy in Large Scale Networks	Precision, Degree & Secrecy rate	This paper explains the issues of wireless network security using Information Theoretic System.
12	APR 2011	Jing Huang, Et al.	Robust Secure Transmission in MISO Channels based on Worst-case	Secrecy rate , Power allocation	This paper investigates the problem of secured data transmission in cryptography using

			Optimization		MISO wiretap channel.
13	JUN 2011	Xiangyun Zhou, Et al.	On the Throughput Cost of Physical Layer Security in Decentralized wireless network	Transmission capacity, Throughput	This paper studies about security issues of decentralized wireless network in single point to point communication using multi antenna transmission.
14	MAY 2012	Yeow-Khiang chia, et al.	Three-Receiver Broadcast channels with common and confidential messages	Security rate, Equivocation rate, Secrecy capacity	This paper describes network security level while transmitting confidential messages over wireless network using artificial noise generation.
15	JUN 2012	HirleyAlves, Et al.	Performance of Transmit Antenna Selection Physical Layer Security schemes	Secrecy capacity, Performance, Power allocation, Secrecy outage probability	This paper investigates the performance of network security during data transmission using multiple antenna system in TAS(Transmitter Antenna Selection)
16	JAN 2013	Nan Yang, et al.	Transmit Antenna Selection for Security Enhancement in MIMO Wiretap channels	Secrecy rate, secrecy capacity, Performance, Transmission power	This paper explains about network security enhancement in single antenna system using TAS.
17	JAN 2013	Giovanni Geraci, Et al.	Secrecy rates in Broadcast channels with confidential Messages and External eavesdroppers	Secrecy capacity, Secrecy rates, Secrecy outage probability	This paper studies about the network security rate while transmitting confidential messages over broad channels using artificial noise generation.
18	MAY 2013	Nuwan S. Ferdinand, et al.	Effects of Out-dated CSI on the Secrecy Performance of MISO Wiretap channels with Transmit Antenna Selection	Secrecy capacity	This paper investigates the effect of network security performance in multiple antenna system using TAS.
19	MAY 2013	Ghadamali Baghe-rikaram, et al.	Secrecy capacity region of Gaussian Broadcast channel.	Equivocation rate, Secrecy capacity, Secrecy rate, Entropy power	This paper describes the capacity of network security using Gaussian wiretap channel in information theoretic system.
20	JAN 2014	AmitavMukherje, et al.	Principles of Physical Layer Security in Multiuser Wireless Networks	Performance, Secrecy capacity	This paper explains the physical layer security using information theoretic system.

Table 2:. Measurements Taken in Aodv Routing Protcol

SNO	YEAR	AUTHOR	TOPIC	MEASUREMENTS	APPLICATIONS	EXISTING SYSTEM	PROPOSED SYSTEM
1	2000	Elizabeth M. Royer, et al.	An Implementation study of the AODV routing protocol	Routing overhead	Data routing	Ad hoc proactive routing protocol	AODV routing protocol
	2001	Sonali Bhargava, et al.	Security Enhancements in AODV protocol for wireless Ad hoc networks	Routing load, Packet delay, Accuracy, Throughput, Packet delivery & Routing overhead	Secured routing in Military operations	Multi hop routing schemes	AODV routing protocol
3	2007	Asad Amir Pirzada, et al.	Multi – linked AODV Routing protocol for wireless Mesh network	Performance, Routing Overhead, Interference rate & Packet delivery	Routing	Multi hop wireless network	AODV – ML (Multi-Link)
4	2007	Asad Amir Pirzada, et al.	High performance AODV routing protocol for Hybrid wireless Mesh Network	Packet delay, Throughput & Packet loss	Secured Routing	Standard AODV routing	AODV – HP (Hybrid Routing)
5	2008	Ahed M. Alshanyour, Et al.	Bypass AODV: Improving Performance of Ad hoc On-demand Distance Vector (AODV) routing protocol in wireless Ad hoc Networks	Node density, Node mobility & Performance	Routing	AODV routing (Unidirectional routing)	Bypass AODV routing
6	2009	Mehdi Medadiah, et al.	Combat with Black Hole attack in AODV routing protocol in MANET	Path rate, Packet delivery & Performance	Routing security	Proactive routing protocol -DSDV (Destination Sequence Distance Vector)	Reactive routing protocol-AODV
7	2009	Hidehisa Nakayama, et al.	A dynamic Anomaly Detection scheme for AODV – Based	Projection distance & Forgetting curve	Secured routing in Disaster, Military	ryptography with proactive routing protocol	MANET routing protocol -Anomaly detec-

			mobile Ad hoc networks		& Entertainment Industry		tion: AODV routing
8	2012	Mehdi Barati, et al.	Performance evaluation of energy consumption for AODV and DSR routing protocols in MANET	Route delay, Routing overhead, Packet delivery&Performance	Secured routing	Proactive routing methods	Reactive routing (AODV & DSR routing)
9	2013	Sheng Liu, et al.	Research of AODV routing protocol for Ad hoc networks	Performance, Average delay, Routing overhead & Packet delivery ratio	Routing repair	Multi hop Ad hoc networks	AODV routing protocol

Table 3: Algorithms Used in Existing Research Works recommendations for AODV Routing with Cryptographic Algorithm

Algorithm	Operation	Status	Alternative
Data Encryption Standard	Encryption	No adequate security	Advanced Encryption Standard
3 Data Encryption Standard	Encryption	Acceptable security level	Advanced Encryption Standard
Rivest Cipher 4	Encryption	No adequate security	Advanced Encryption Standard
Advanced Encryption Standard -CBC mode	Encryption	Provide adequate security	Advanced Encryption Standard –GCM
Advanced Encryption Standard -GCM mode	Authenticated encryption	Next generation encryption	
Diffie-Hellman 768 -1024 Rivest–Shamir–Adleman 768 - 1024 Digital Signature Algorithm 768-1024	Key exchange Encryption Authentication	No adequate security	Diffie-Hellman -3072 (Group 15) Rivest–Shamir–Adleman-3072 Digital Signature Algorithm -3072
Diffie-Hellman -2048 Rivest–Shamir–Adleman -2048 Digital Signature Algorithm -2048	Key exchange Encryption Authentication	Provide adequate security	Elliptic-curve Diffie–Hellman -256 Elliptic Curve Digital Signature Algorithm -256
Diffie-Hellman -3072 Rivest–Shamir–Adleman -3072 Digital Signature Algorithm -3072	Key exchange Encryption Authentication	Provide adequate security	Elliptic-curve Diffie–Hellman -256 Elliptic Curve Digital Signature Algorithm -256
Message Digest 5	Integrity	No adequate security	Secure Hash Algorithm-256
Secure Hash Algorithm-1	Integrity	Acceptable security level	Secure Hash Algorithm -256
Secure Hash Algorithm -256, 384,512	Integrity	Next generation encryption	Secure Hash Algorithm -384
Hash-based message authentication codes - Message Digest 5	Integrity	Acceptable security level	Hash-based message authentication codes - Secure Hash Algorithm -256
Hash-based message authentication codes - Secure Hash Algorithm-1	Integrity	Provide adequate security	Hash-based message authentication codes - Secure Hash Algorithm -256
Hash-based message authentication codes - Secure Hash Algorithm -256	Integrity	Next generation encryption	Elliptic-curve Diffie–Hellman -384 Elliptic Curve Digital Signature Algorithm -384
Elliptic-curve Diffie–Hellman -256 Elliptic Curve Digital Signature Algorithm -256	Key exchange Authentication	Next generation encryption	
Elliptic-curve Diffie–Hellman -384 Elliptic Curve Digital Signature Algorithm -384	Key exchange Authentication		

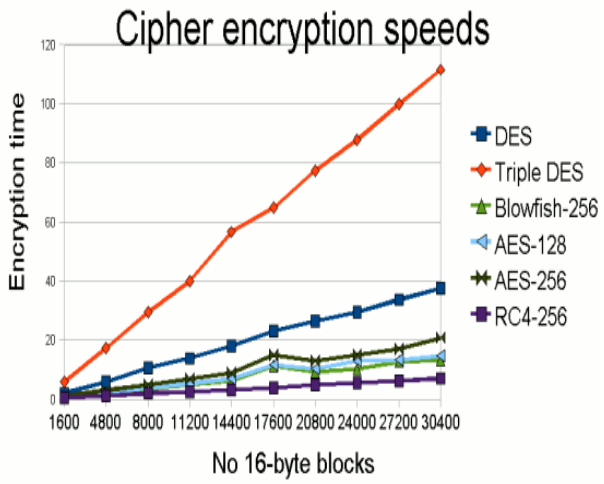


Fig. 1: Speed Of Cryptographic Algorithm.

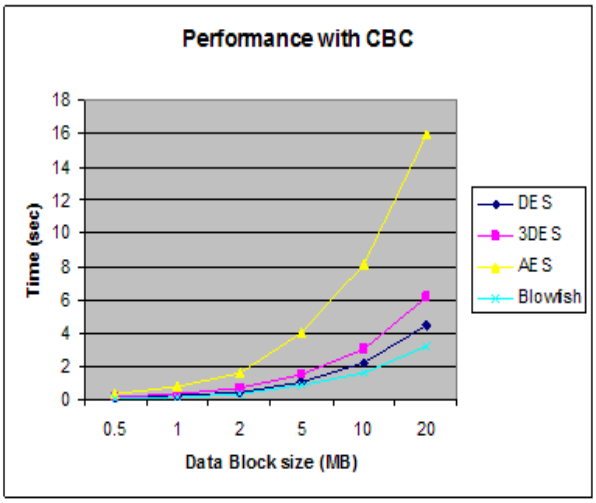


Fig. 2: Performance of Cryptographic Algorithm.

4. Conclusion

In this work, we suggested AODV-BA which deflects route breaks established on AODV in ad-hoc routing protocols. It is the princi-

ple where each intervening node on an active route reveals the vulnerability of the interconnection break to the upstream node planted on four aspects of the received radio, the overlay of paths, the battery and consistency. The route breaks are avoided by re-styling a prime route with our prospective innovation before the route breaks.

References

[1] A. D.Wyner, "Thewire-tapchannel,"Bell Syst.Tech. J., vol.54, no.8, pp. 1355–1387, 1975.

[2] I. Csiszár and J. Körner, "Broadcast channels with confidential messages," IEEE Trans. Inf. Theory, vol. IT-24, no. 3, pp. 339–348, May 1978.

[3] R. Liu, I.Maric, P. Spasojevic, andR. D. Yates, "Discrete memory less interference and broadcast channels with confidential messages: Secrecy rate regions," IEEE Trans. Inf. Theory, vol. 54, no. 6, pp. 2493–2507, Jun. 2008.

[4] G.Bagherikaram, A.S.Motahari, A.K.Khandani, "Secure-broadcasting: The secrecy rate region," in Proc. 46th Annu. Allerton Conf. Commun., Control Comput. Sep. 2008, pp. 834–841.

[5] A. Khisti, A. Tchamkerten, and G. Wornell, "Secure broadcasting over fading channels," IEEE Trans. Inf. Theory, vol. 54, no. 6, pp. 2453–2469, Jun. 2008.

[6] Royer, Elizabeth M., and Charles E. Perkins. "An implementation study of the AODV routing protocol." *Wireless Communications and Networking Confernce, 2000.WCNC.2000 IEEE*.Vol. 3. IEEE, 2000.

[7] Bhargava, Sonali, and Dharma P. Agrawal. "Security enhancements in AODV protocol for wireless ad hoc networks." *Vehicular Technology Conference, 2001. VTC 2001 fall. IEEE VTS 54th*.Vol. 4. IEEE, 2001.

[8] Gwalani, Sumit, Elizabeth M. Belding-Royer, and Charles E. Perkins. "AODV-PA: AODV with path accumulation." *Communications, 2003.ICC'03.IEEE International Conference on*.Vol. 1. IEEE, 2003.

[9] Pirzada, Asad Amir, Ryan Wishart, and Marius Portmann. "Multi-linked AODV routing protocol for wireless mesh networks." *Global Telecommunications Conference, 2007.GLOBECOM'07.IEEE*.IEEE, 2007.

[10] Pirzada, Asad Amir, and Marius Portmann. "High performance AODV routing protocol for hybrid wireless mesh networks." *Mobile and Ubiquitous Systems: Networking & Services, 2007. MobiQuitous 2007.Fourth Annual International Conference on*.IEEE, 2007.

[11] Medadian, Mehdi, Mohammad HosseinYektaie, and Amir MasoudRahmani. "Combat with Black Hole Attack in AODV routing protocol in MANET." *Internet, 2009.AH-ICI 2009.First Asian Himalayas International Conference on*.IEEE, 2009.

[12] Alshanyour, Ahed M., and UthmanBaroudi. "Bypass AODV: improving performance of ad hoc on-demand distance vector (AODV) routing protocol in wireless ad hoc networks." *Proceedings of the first international conference on ambient media and systems*. ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering), 2008.

[13] Nakayama, H., Kurosawa, S., Jamalipour, A., Nemoto, Y., & Kato, N. (2009). A dynamic anomaly detection scheme for AODV-based mobile ad hoc networks. *IEEE transactions on vehicular technology*, *58*(5), 2471-2481.

[14] Barati, Mehdi, KayvanAtefi, FarshadKhosravi, and YasharAzabDaftari. "Performance evaluation of energy consumption for AODV and DSR routing protocols in MANET." In *Computer & Information Science (ICCIS), 2012 International Conference on*, vol. 2, pp. 636-642.IEEE, 2012.

[15] Liu, Sheng, Yang Yang, and Weixing Wang. "Research of AODV routing protocol for ad hoc networks1." *AASRI Procedia* 5 (2013): 21-31.

[16] ZhouLidong and Zygmunt J. Haas. "Securing ad hoc networks." *IEEE network* 13.6 (1999) 2430.

[17] Gupta, Piyush, and Panganmala R. Kumar. "The capacity of wireless networks." *IEEE Transactions on information theory* 46.2 (2000): 388-404.

[18] Anand, Santhanakrishnan, and RajarathnamChandramouli. "On the location of an eavesdropper in multiterminal networks." *IEEE Transactions on Information Forensics and Security* 5, no. 1 (2010): 148-157.

[19] Zhou, Xiangyun, and Matthew R. McKay. "Secure transmission with artificial noise over fading channels: Achievable rate and optimal power allocation." *IEEE Transactions on Vehicular Technology* 59.8 (2010): 3831-3842.

[20] Pinto, Pedro C., João Barros, and Moe Z. Win. "Wireless secrecy in large-scale networks." *Information Theory and Applications Workshop (ITA), 2011*.IEEE, 2011.

[21] Huang, Jing, and A. Lee Swindlehurst. "Robust secure transmission in MISO channels based on worst-case optimization." *IEEE Transactions on Signal Processing* 60.4 (2012): 1696-1707.

[22] Chia, Yeow-Khiang, and Abbas El Gamal. "Three-receiver broadcast channels with common and confidential messages." *IEEE Transactions on Information Theory* 58.5 (2012): 2748-2765.

[23] Yang, N., Yeoh, P. L., Elkashlan, M., Schober, R., &Collings, I. B. (2013). Transmit antenna selection for security enhancement in MIMO wiretap channels. *IEEE Transactions on Communications*, *61*(1), 144-154.

[24] Ferdinand, Nuwan S., Daniel Benevides da Costa, and MattiLatva-aho. "Effects of outdated CSI on the secrecy performance of MISO wiretap channels with transmit antenna selection." *IEEE Communications Letters*17.5 (2013): 864-867.

[25] Mukherjee, A., Fakoorian, S. A. A., Huang, J., &Swindlehurst, A. L. (2014). Principles of physical layer security in multiuser wireless networks: A survey. *IEEE Communications Surveys & Tutorials*, *16*(3), 1550-1573.

[26] Deepa.A, Ramkumar.S," Active Resource and Job Allocation for Power Minimization in Mobile Cloud Systems", International Journal of Advanced Research Trends in Engineering and Technology, Vol.3 (12), pp.57-63, Mar-2016.

[27] Sibi.V, Ramkumar.S," Privacy Reserving in Multimedia Big Data Using Secure Data Repository System", International Journal of Advanced Research Trends in Engineering and Technology, Vol.3 (17), pp.01-10, Mar-2016.