Security in Multi-hop Wireless Networks

[1]Amardeep Singh, [2]Gurjeet Singh
[1]Department of Computer Sc. & Engg., SVIET, Ramnagar, Banur, Punjab, India
[2]Department of Computer Sc. Engineering, DBIEM, Moga, Punjab, India

Abstract

Multi-hop wireless networks are facing some research issues regarding routing protocols and security mechanisms. Multi-hop decentralized architecture, media access delay, lower link life, and multi-layer security threats are the key challenges which need to be address. The selection of optimal path for routing and the detection of multilayer security attacks cannot be achieved with the traditional approaches. Cross layer design is the only solution to cope with these kinds of challenges in multi-hop wireless networks. In this paper, we discuss the importance of cross layer security mechanisms and routing protocols for multi-hop wireless networks by critical comparison.

Keywords
Multi-hop, security, cross layer design.

I. Introduction

The change in technologies from wired to wireless networks opened new doors for research. Wireless networks for mobile and broadband applications have emerging and growing trends. Such kind of fast changes in communication technologies and emerging trends stress to optimize the performance of the multi-hop wireless networks. However, the OSI stack which is responsible for end to end communication was primarily designed for wired networks, which cannot perform well in multi-hop wireless networks, as the higher layers and their residing protocols remained unaware of the underlying protocols. Multi-hop wireless networks impose new challenges such as, the varying nature of the signal strength, higher bit-error rates, dynamic variations in channel quality, fading effects, interference problems, mobility, shared and contention based MAC, multi-hop transmission and path selection at network layer needs some degree of interaction amongst different layers so that to optimized the overall network performance. In order to solve such problems, cross layer information exchange is proposed in[7,8].

The basic purpose of cross layer design is to use multilayer parameters from OSI stack to increase the efficiency and performance of multi-hop wireless networks. Cross layer design approach can be used to improve the overall performance of multi-hop wireless networks such as wireless sensor networks (WSN), mobile ad hoc networks (MANET), and wireless mesh networks (WMN). For example:

- In WSNs and MANETs, battery power can be saved using intelligent cross layer mechanism, which ensure to turn on the radios only when it sense some sort of transmission.
- QoS routing which are aware of link life and bandwidth can be implemented, which selects an optimal route having more link life and more bandwidth.
- In wireless mesh networks, QoS can be improved for multimedia applications, efficient scheduling and utilization of network resources.

Beside the problems of battery power, QoS routing, MAC scheduling, and efficient utilization of network resources, multi-hop wireless networks are more vulnerable to different security risks due to inherent attack prone features such as shared MAC, multi-hop decentralized architecture, wireless medium etc. The attackers can exploit these features to bring serious disorders and routing disruption. Furthermore, multi-hop wireless networks are exposed to multi-layer threats. A security mechanism for one layer cannot protect the other layer. Hence cross layer security mechanisms are indeed necessary to protect these multi-hop wireless networks from passive, active and denial of service attacks.

II. Cross layer parameters for routing

In [9], cross layer architecture is proposed with different parameters at different layers. More optimized algorithms can be design by allowing Physical and MAC layers to provide information to Network and transport layers regarding:

- Physical layer information can be used for power control, signal strength, interference and noise ratio
- At MAC layer, some information can be analyzed such as contention, fairness, scheduling, media access delay, throughput and bandwidth.
- Network layer can facilitate in optimal path selection based on information received from PHY and MAC layers.
- Transport layer can be considered for congestion control.

The different layers and the associated parameters are given in Fig. 1.

These different parameters can be intelligently exchanged in multi-hop wireless networks to select a route which has:

- More link life, good signal strength, less interference and noise ratio
- Less media access delay, more bandwidth and throughput
- Less congestion

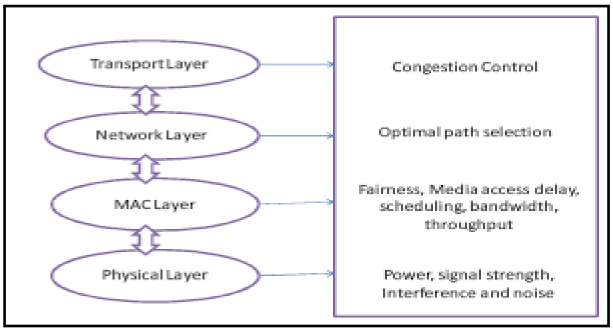
Transport Layer
Congestion Control
Network Layer
Optimal path selection
MAC Layer
Fairness, Media access delay, scheduling, bandwidth, throughput
Physical Layer
Power, signal strength, Interference and noise

Fig. 1: Layers and associated parameters

Such kind of parameters needs to be considered before the design of any routing protocol for multi-hop wireless networks. Most of the current routing protocols such as AODV, DSR etc select the shortest path between source and destination. Now, the issue is, if this shortest path has such intermediate nodes having less battery power, more delay, less bandwidth, high congestion, more noise ratio. In such cases, the path is not optimal for long and bandwidth oriented transmissions such as multimedia or real time applications, as such applications need more bandwidth, less delay and more link life. An adaptive and optimal route can only be designed using cross layer approach, in which the source and destination select route on the basis of many parameters form different layers. An application specific adaptive routing protocol can also be devised for multi-hop wireless networks. However selection of appropriate parameters and information exchange amongst different layers is a challenging research issue.

Cross layer protocols perform well as compared to traditional. The comparison of On-Demand Link Weight (ODLW) [3] and AODV [4,5] is given in this section. AODV is one of the benchmark routing protocol for MANET. AODV keeps one-hop information in the routing table and select the shortest path between source and destination. The metric used is hop count in AODV. On the other hand, ODLW is a cross layer routing protocol, in which the path selection is based on link weight parameters such as high bandwidth, minimum delay and more battery power. Furthermore, the route selection process is adaptive in nature, keeping in view the requirements of applications.

Route discovery efficiency is very important factor, and the comparison of ODLW and AODV is given in Fig. 2. This factor shows how long the routing protocol takes for discovering a certain route from source to destination. AODV has a lot of acknowledgement packets as compared to ODLW, so routing time is significant larger than the ODLW.

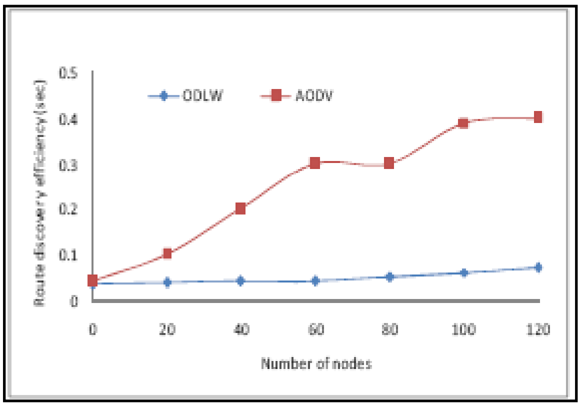

Fig. 2: Route discovery time

The next parameter that is under consideration is the effect of increasing traffic on the routing overhead as shown in Fig. 3. AODV has more routing overhead as compared to ODLW due to a lot of hello messages and acknowledgements.

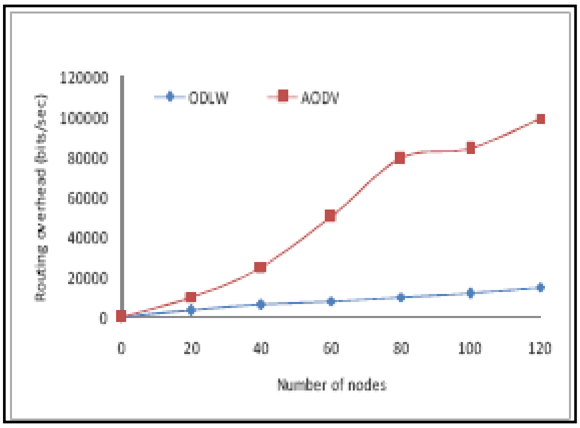

Fig. 3: Routing overhead

The comparison of AODV and ODLW is given in Table 1.

Table 1: Comparison of ODLW & AODV

	ODLW	AODV
On-demand route selection	Yes	Yes
Alternative route	Yes	Yes
Network size	All sizes	Large
Routing path	Adaptive	Shortest
Link reliability	Yes	No
Network load	Low	High
Routing overhead	Low	High
Application adaptive	Yes	No

III. Cross layer parameters for Security

Multi-hop wireless networks are more unsafe as compared to wired or single hop wireless networks. The security threats at different layers are shown in Fig. 2.

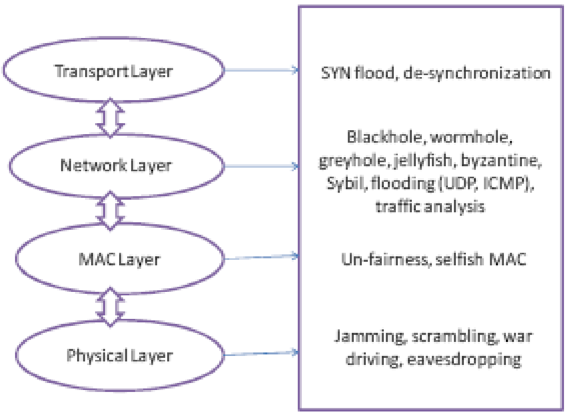
Transport Layer
Network Layer
MAC Layer
Physical Layer
SYN flood, de-synchronization
Blackhole, wormhole, greyhole, jellyfish, byzantine, Sybil, flooding (UDP, ICMP), traffic analysis
Un-fairness, selfish MAC
Jamming, scrambling, war driving, eavesdropping

Fig. 4: Multilayer security attacks

Such kind of multi-layer security attacks need to be considered before the design of any security mechanism or intrusion detection system. Most of the current intrusion detection systems detect security risks at network layer in multi-hop wireless networks. To detect multi-layer security attacks, the only option is to consider cross layer design. Two approaches can be adapted for designing cross layer security mechanism for multi-hop wireless networks. One is multiple-inputs single analysis (MISA), in which the system gathers multiple inputs from different sources (layers) and analyzes these inputs in a single analysis engine to make a decision. Second option is multiple-inputs multiple analysis (MIMA). In MIMA, the system obtains multiple inputs from different layers, and these inputs are analyzed separately in different analysis engines. However, for WSNs and MANETs, MISA is more appropriate as it consume less resources. However, the selection of proper parameters and the interaction of different layers to exchange information to detect multi-layer attacks is a complex and challenging research issue.

Cross layer security mechanisms perform well as compared to traditional approaches. Flooding is one of the most severe security threats in multi-hop wireless networks. The basic purpose of flooding attacks is to congest the network with unnecessary packets. If the severity of flooding attack is less than the network resources, then it would slow down the network performance. However, if the severity of flooding attack is more than the network resources such as bandwidth may bring down the entire network [6]. Furthermore, multi-hop wireless networks such as WMN is vulnerable to MAC layer flooding attacks such as probe request flood [2]. In this section, we compared two flood detection mechanisms; one is based on traditional approach [1], while the other is based on cross layer design approach. The traditional approach is capable to detect TCP/IP floods such as SYN, UDP and IGMP. On the other hand, the cross layer approach is capable to detect the MAC layer flooding attacks too. The comparison of both approaches is given in Table 2.

Table 2: Comparison of Cross layer and Traditional Flood detection mechanism

	Cross layer approach	Traditional approach
SYN Flood detection	Yes	Yes
UDP Flood detection	Yes	Yes
ICMP Flood detection	Yes	Yes
IGMP Flood detection	Yes	Yes
Probe Flood detection	Yes	No
De authentication flood detection	Yes	No
Hello flood detection	Yes	No

IV. Conclusions

Efficient and robust routing and implementation of reliable security mechanism in multi-hop wireless networks is a challenging task. Routing protocols in multi-hop environment must consider some parameters such as path life, path bandwidth, link delay so that to adaptively select the most optimal path. Similarly, the multi-layer security issues and attacks must be considered before proposing any security mechanism for multi-hop wireless networks. Cross layer design is the only possible way to cope with multilayer security attacks and to propose an adaptive routing protocol.

References

[1] S. Noh, G. Jung, K. Choi, C. Lee, “Compiling network traffic into rules using soft computing methods for the detection of flooding attacks,” Elsevier, Applied Soft Computing, Vol. 8, 1200- 1210, 2008.

[2] S. Khan, K-K. Loo, “Real-time cross-layer design for large-scale flood detection and attack trace-back mechanism in IEEE 802.11 Wireless Mesh Networks,” Elsevier Network Security, Vol. 2009, Issue 5, pp. 9-16, May, 2009.

[3] A.N. Al-Khwildi, S. Khan, K.K. Loo, H.S. Al- Raweshidy, ”Adaptive Link-Weight Routing Protocol using Cross-Layer Communication for MANET”, WSEAS Transactions on Communications, Volume 6, Issue 11, pp. 833-839, 2007.

[4] C. Perkins, E.M. Royer, “Ad-hoc on-demand distance vector routing,” WMCSA Second IEEE Workshop, pp. 90 – 100, 1999.

[5] C. Perkins, E.M. Royer, S.Das, “Ad-hoc on demand distance vector (AODV) routing, IETF, RFC 3561, 2003.

[6] S. Khan, N. Mast, K-K. Loo, “Denial of service attacks and mitigation techniques in IEEE 802.11 Wireless mesh networks,” Information: an International Interdisciplinary Journal, Vol. 12, No. 1, January 2009.

[7] Shakkottai, S., Rappaport, T.S., Karlsson, P.C.,”Cross-layer design for wireless networks”, Communications Magazine IEEE, vol 41, no 10, pp 74 - 80 , Oct 2003.

[8] Srivastava, V.; Motani, M.,”Cross-layer design: a survey and the road ahead”, Communications Magazine IEEE, vol 43, no12, pp112 - 119, Dec. 2005.

[9] [Online] Available : http://www.ibcn.intec.ugent.be/2007/Hybrid%20Wir eless%20Mesh%20Networks.pdf.

Er.Amardeep Singh is working as Associate Professor-CSE., S.V.I.E.T., Banur and is also performing the job of Head of Computer Sc. & Engineering. and Head of the Department in Swami Vivekanand Research & Technology Park. Er.Amardeep Singh has done B.Tech in Computer Science & Engg. & M.Tech. in Information Technology from Guru Nanak Dev University Campus, Amritsar. He has also done Masters in Business Administration as dual specialization in Marketing & Human Resource Management. Now he is pursuing Ph.D. in Computer Sciences. His area of interest is Computer Networks, Parallel & Distributed Computing. He is the life member of Indian Society for Technical Education (I.S.T.E.) and has published & presented 38 papers in International/National Journals & Conferences, He has also written & published 10 highly acclaimed books. He has attended & organized various Short Term/FDP/Workshop programs. He has Teaching & Industry Experience of more than 9.

Er.Gurjeet Singh is a dynamic researcher and prolific author in the field of Computer Engineering. He did his M.Tech (CSE) from lovely Professional University Phagwara. Currently he is working as the Head, Dept. Of Computer Science, DBIEM,Moga. His research interest is in Wireless Networks & Network Security. He is a life member of ISTE and has published 25 National & International research papers in journals and conferences. He has written 10 highly acclaimed text & research books.