Middle-East Journal of Scientific Research 22 (7): 1072-1076, 2014
ISSN 1990-9233

DOI: 10.5829/idosi.mejsr.2014.22.07.21968

Detection of Selfish and Malicious Node in Wireless Mesh Network Using Pana Protocol

[1]G. Michael, [1]A.R. Arunachalam and [2]A. Chandrasekar

[1]Department of Computer Science and Engineering, Bharath University Chennai, Tamilnadu, India
[2]Professor, St. Joseph College of Engineering Chennai, Tamilnadu, India

Abstract: Wireless Mesh Network is one of emerging technology of the next generation networks. All the routing protocols in WMNs assume all nodes to be co-operative in forwarding each other's packets. However, a node might try to save its energy by dropping others packet. The proposed mesh network is divided into clusters which reduce the traffic congestion to the gateway. Each cluster has cluster head which performs collection of node details and also monitors the behaviour of each node. The detection phase is used to find selfish nodes in WMNs. Authenticating the node in the network is a key point of network security. Using Protocol for carrying Authentication for Network Access authentication, nodes in wireless mesh network are authenticated to detect malicious node.

Key words: Wireless Mesh Networks · WMN Security · Selfish nodes · Clustering · Node misbehavior · Threshold Authorization · PANA · EAP-TTLS

INTRODUCTION

Wireless mesh architecture provides an effective high-bandwidth networks over a specific area. A wireless mesh network made up of radio nodes organized in a mesh topology [1]. Wireless mesh networks consist of mesh clients, mesh routers and gateways. The mesh clients are laptops, cell phones and other wireless devices.Mesh routers forward data to and from the gateways. Intermediate nodes not only boost the signal, but cooperatively make forwarding decisions based on their knowledge of the network [2].

In this paper, the architecture enforces cooperation between nodes by detecting selfish routers from the network. The contributions of the scheme are: (a) It detects the presence of selfish routers/nodes. (b) The architecture is divided into clusters to reduce the communication overhead. The Authentication scheme used is PANA. PANA uses similar authentication scheme as 802.1X and is independent of the underlying access technologies. It is applicable to any network topology and aims at offering [3].

Architecture of WMN: The components of a WMN include mesh clients, mesh routers and gateways. Mesh routers form the wireless backbone providing services to the mesh clients by forwarding packets to and from the Internet. WMNs often have one or more mesh gateways which provide backhaul connectivity to the Internet [4].

Figure 1 illustrates that the mesh routers form an infrastructure for clients. The mesh routers form a mesh of self-configuring, self-healing links among themselves. With gateway functionality, mesh routers can be connected to the Internet.

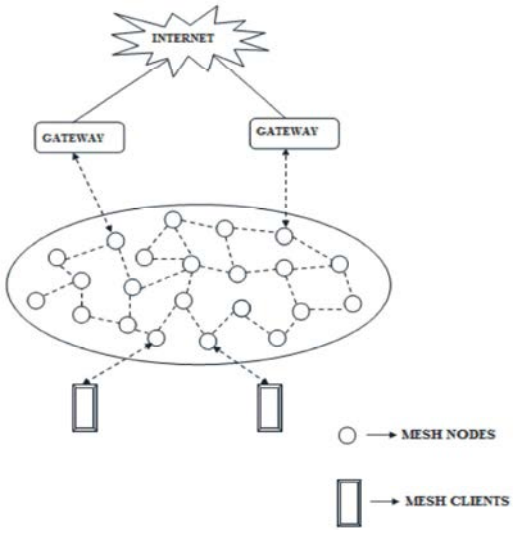

Fig 1: Wireless Mesh Network

Corresponding Author: G. Michael, Department of Computer Science and Engineering, Bharath University Chennai, Tamilnadu, India. E-mail: micmgeo@yahoo.co.in.

Related Work: This section gives a brief review on existing techniques for detecting selfish node from wireless mesh network [5].

Mitigating Routing Misbehavior: Reputation based schemes observe the behavior of their neighbouring nodes through promiscuous overhearing and accordingly assign them a reputation rating which are used for identifying the selfish nodes. Nodes often have components such as watchdog [2] which buffers all packets before transmission and then overhears its neighbour's transmission to check whether it is forwarded or not. Results from the watchdog component are fed to the reputation systems which update the reputation ratings on network nodes based on their cooperation and participation in packet forwarding [6].

Reputation values can be periodically shared by different reputation components and nodes with low ratings are excluded or their packets denied forwarding. However, such schemes cannot be applied to wireless mesh networks due to their multi-channel characteristics. This is because a watchdog component tuned to a certain channel cannot observe communication on other channels. Moreover promiscuous monitoring cannot differentiate between intentional packet drop and packet drop due to a transmission collision [7].

Distributed-Self Policing Architecture for Fostering Node Cooperation: In the scheme every mesh router sends periodic traffic reports to the sink nodes. To enforce cooperation, selfish mesh routers are excluded from the network after a certain number of offences.The sink nodes apply a set of forwarding rules to isolate a selfish node based on the number of times it is caught in selfish acts [4]. The scheme is independent of the routing protocol or network architecture and is suitable for multi-channel wireless mesh network.

D-SAFNC does not require a central auditing server since it uses the mesh gateways to aggregate and process traffic reports from nodes. With the increase in the number of mesh routers, the traffic caused by reporting nodes can congest the gateways and hence hamper the network performance.

Link Quality in Multi-hop WMN: The use of link quality metric is to differentiate between intentional packet drop and packet drop due to poor link quality.

Broad-cast based Active Probing (BAP) has been widely used for link-quality aware routing. Although it incurs a small overhead, broadcasting does not always generate the same quality measurements as actual data. Thus, BAP provides inaccurate link-quality measurements [3]. Moreover, its use of an identical type of probing in both directions of a link generates bi-directional results. Unicast based probing provides accurate and uni-directional results owing to its resemblance to the use of actual data transmissions, but it incurs significant overheads. Finally, passive monitoring is the most efficient and accurate since it uses actual data traffic. However, it also incurs the overhead of probing idle links.

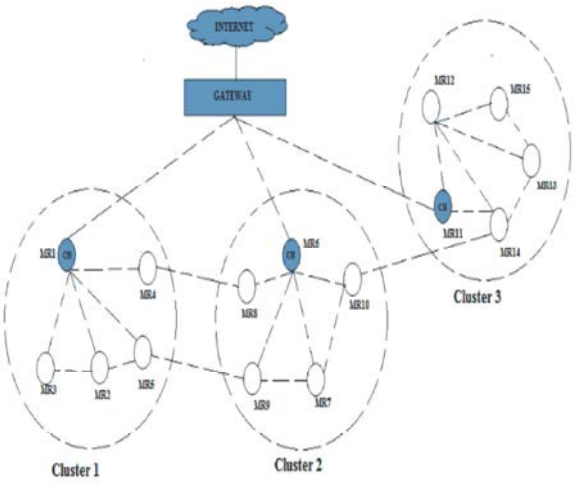

Fig 2: Mesh Routers divided into clusters

Clustering Scheme in WMN: The architecture consists of monitoring agents and sink agents. The Monitoring Agents (MA) collect traffic reports from the neighbouring mesh routers. They are hosted by the cluster head and the sink agents are hosted in the gateway to perform the operations like detection and elimination of selfish node from the network. Fig. 2 shows the cluster based architecture of the proposed scheme. The mesh routers are grouped into clusters and one mesh router in each cluster is chosen as a cluster-head [1]. This greatly reduces the communication overhead of the detection scheme compared to other schemes.

Cluster heads are selected based on their lowest network Ids. All the mesh routers in the network broadcast a "HELLO" message which contains their network IDs to identify the presence of neighbouring router. Based on this information, the lowest network IDs are selected as a cluster-head. Once the cluster head is selected, it broadcast the message which contains the distance from its orgin to the neighbouring node. Based on this, the neighbouring node joins with the neighbouring cluster and forms a group.

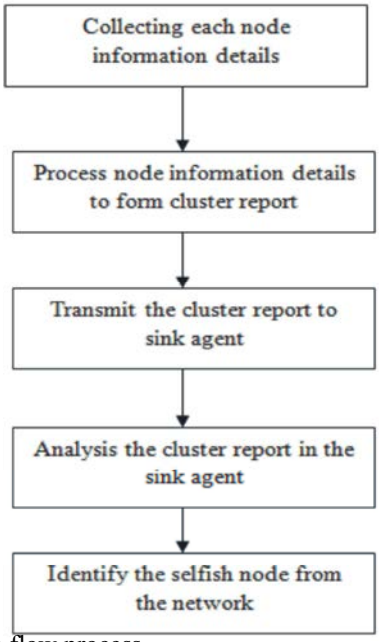

Fig 3: Data flow process

Description of Flow Process: Fig.3 shows the flow of data transmission between Monitoring Agent and Sink Agent (SA). All the mesh router/node information's are collected by the cluster head and then processed to form a cluster report. The generated cluster report is transmitted from the cluster-head to the sink agent [1]. Once the cluster report is gathered, they are analyzed. Based on the report generated each node will be given a rating and all the node information's are stored in a table. The SA uses the report to eliminate the selfish mesh router from the network.

Protocol for Performing Authentication for Pana Framework: The Internet Engineering Task Force (IETF) has been working since 2001 to evolve a medium independent solution that enables EAP messages to be carried over IP within a protocol for carrying authentication for network access. As a consequence, PANA is designed for mutual authentication and fast re-authentication that carries information by using Attribute Value Pairs (AVPs) [5]. This section explains the PANA framework and its security mechanisms.

Architectural Model: A new client, joining the network gets an IP address called pre-PANA address from the local Dynamic Host Configuration Protocol (DHCP) [6] server and initiates PANA to start the authentication process. PANA comprises of following functional entities (Illustration in Fig. 2):

PANA Client (PaC): It represents the client domain of PANA which resides in an access device i.e. PC, PDA or Laptop, etc. It submits its credentials to PANA Authentication Agent (PAA) over PANA protocol to gain access to the network.

PANA Authentication Agent (PAA): This entity resides in the access network and performs the task of verifying credentials forwarded by PaC. It interacts with AS to enforce network access control through an Enforcement Point (EP) / AP. PAA by definition is placed at a single IP hop distance from PaC. The PAA and EP/AP can be physically co-located in a single device.

Enforcement Point (EP): It does not allow network access to a new client until it is authenticated and authorized. Before authentication, only the traffic meant for DHCP server for the purpose of configuring the new client is allowed. It comprises of filters provided by PAA to apply enforcement policies to every packet in the incoming and outgoing traffic from a network.

Authentication Server (AS): It is the back end main authentication server, a part of AAA mechanism, which ultimately authorizes a new client to gain network access. It is approached by the PAA for confirmation of the client's credentials which are stored in its database. Normally RADIUS or Diameter is used for the purpose. PAA and AS can be physically co-located.

Functional Overview: Authentication of a new PaC to a PAA depends on the credentials verification performed by an AS which communicates access control state to the EP. PANA runs between PaC and PAA and transports EAP authentication method, using UDP as transport layer protocol. Choice of EAP method depends on the credentials used by the PaC and the AS. In most cases, PANA authentication involves a distant AAA server i.e. RADIUS or Diameter that communicates with the PAA using an AAA protocol. PANA comprises of four main phases namely Discovery and Handshake, Authentication and Authorization, Access and finally theTermination phase (Fig. 4)

Security Mechanisms Embedded in PANA: PANA offers embedded mechanisms to counter security threats like passive eavesdropping, message relaying, message distortion, man in the middle, active impersonation and DoS attacks etc [7].

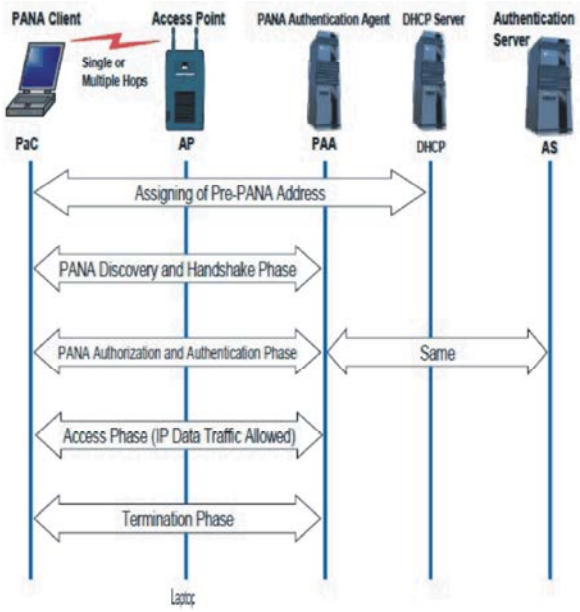

Fig 4: PANA Frame work and overall phases

Message Sequence Numbers: Each PANA message carries a sequence numbers which monotonically increases by one after every new request message. The sequence numbers not only perform orderly delivery of EAP messages and eliminate duplication, but also prevent spoofing in ongoing PANA and EAP sessions.

Cookie Based Scheme: The discovery and handshake phase is prone to spoofing attacks by a malicious node as there is no security relationship between PAA and PaC at that stage. To avert these basic DoS attacks, a cookie is added to the PANA-Start-Request message to ensure delivery of messages to the correct IP address.

Message Integrity: The PANA Security Association (SA) created at the end of a successful authentication provides message integrity and particularly protects the PaC's identifier and thereby prevents the service theft attack.

Periodic Re-Authentication: PANA architecture uses periodic re-authentication which ensures that the IP spoofing (if any) is effective only for a small duration.

Message Authentication Code (MAC): The EAP success or failure messages transmitted by PAA to PaC at the end of the authentication process are protected by a MAC. This prevents attackers from launching DoSattacks against the PaC by sending a spoofed EAP failure message.

Traffic Confidentiality: PANA does not provide traffic confidentiality by itself but it bootstraps a confidentiality protocol at link or IP level i.e. 802.11i or IPSec, respectively. On successful authentication, the data traffic is allowed which is protected by one of these protocols. IPSec is considered more feasible as it not only exercises strong access control by authenticating packet's origin but also provides data encryption thus, ensuring protection against eavesdropping, message distortion and active impersonation.

CONCLUSION

In this paper, the architecture model explains about the detection process of selfish node in wireless mesh networks. The clustering scheme reduces the traffic congestion in the network. The behaviour of mesh routers is monitored by collecting traffic reports periodically. The SAs process the reports to detect selfish nodes. Also security is a main issue in the wireless mesh network. Using threshold based authentication, it is possible to establish a scheme in wireless mesh network to restrict the entry of malicious node based on threshold number of nodes allow a new node to enter in the network. Use PANA ensures authentication and authorization for network access and services in multi-hop WMNs and to restrict the selfish and Malicious network.

REFERENCES

1. Saxena Nikhil, Mieso Denko and Dilip Banerji, 2010. A hierarchical architecture for detecting selfish behaviour in community wireless mesh networks, Elsevier, Computer Communication.
2. Marti, S., T.J. Giuli, K. Lai and M. Baker, 2000. Mitigating routing misbehavior in mobile ad hoc networks, in: Proceedings of the Sixth Annual International Conference on Mobile Computing and Networking, pp: 255-265.
3. Kim and K.G. Shin, 2006. On accurate measurement of link quality in multi-hop wireless mesh networks, in: Proceedings of the 12th Annual International Conference on Mobile Computing and Networking, MOBICOM, pp: 38-49.
4. Santhanam, L., N. Nandiraju, Y. Younghwan and D.P. Agrawal, 2006. Distributed selfpolicing architecture for fostering node cooperation in wireless mesh networks, in: Proceedings of the 11th International Conference on Personal Wireless Communications, IFIP TC6, PWC 2006, pp: 147-158.

5. Forsberg, D., Y. Ohba, B. Patil and H. Tschofenig, 2006. Protocol for Carrying Authentication and Network Access (PANA), draft-ietf-pana-pana-11 (work in progress).
6. Droms, R., 1997. Dynamic Host Configuration Protocol, IETF RFC 2131.
7. Parthasarathy, M., 2005. Protocol for Carrying Authentication and Network Access (PANA) Threat Analysis and Security Requirements", IETF RFC 4016.