International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
http://www.ijcsjournal.com Volume 5, Issue 1, No 11, 2017 ISSN: 2348-6600
Reference ID: IJCS-210 PAGE NO: 1312-1316
Sri Vasavi College, Erode Self-Finance Wing 3rd February 2017
National Conference on Computer and Communication NCCC'17
http://www.srivasavi.ac.in/ nccc2017@gmail.com

Quality of Secure Video Transmission Using Secure Multicast Routing Algorithm

Ms.G.MENAKA,M.Sc.,M.Phil.,
HEAD, DEPARTMENT OF COMPUTER SCIENCE AND COMPUTER APPLICATIONS,
VIVEKANANDHA ARTS AND SCIENCE COLLEGE FOR WOMEN.
VEERACHIPALAYAM,SANKARI,SALEM-637 303
Ph.No:9442512493 Mail-ID:menaka.guru@gmail.com
&
Dr.N.RAJENDRAN,M.C.A.,M.Phil.,Ph.D.,
PRINCIPAL,
VIVEKANANDHA ARTS AND SCIENCE COLLEGE FOR WOMEN.
VEERACHIPALAYAM,SANKARI,SALEM-637 303
Ph.No:94437345613 Mail-ID:vpnraj@gmail.com

ABSTRACT- The exponential growth of network transmission has created new challenges for the control and administration of large-scale networks, which consist of heterogeneous elements under dynamically changing traffic conditions. These emerging applications need guaranteed service levels, beyond those supported by best-effort networks, to deliver the intended services to the end user. Several models have been proposed for a Quality of Service (QoS) framework that can provide the means to transport these services. It is desirable to find efficient routing strategies that can meet the strict routing requirements of these applications. QoS routing is considered as one of the major components of the QoS framework in communication networks. In QoS routing, paths are selected based upon the knowledge of resource availability at network nodes and the QoS requirements of traffic. Several QoS routing schemes have been proposed that differ in the way they gather information about the network state and the way they select paths based on this information.

The biggest downside of current QoS routing schemes is the frequent maintenance and distribution of global state information across the network, which imposes huge communication and processing overheads. Consequently, scalability is a major issue in designing efficient QoS routing algorithms, due to the high costs of the associated overheads. In this proposed QoS routing has shown promising results in achieving good routing performance, while at the same time eliminating many scalability related problems. The instability and limited resources in the networks to make the video transmission is the challenging task.

Transmission of video streams through secure multipath routing in network can enhance the quality of video transmission.In this transmission first receives as inputs three quality of service

International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
http://www.ijcsjournal.com Volume 5, Issue 1, No 11, 2017 ISSN: 2348-6600
Reference ID: IJCS-210 PAGE NO: 1312-1316
Sri Vasavi College, Erode Self-Finance Wing 3rd February 2017
National Conference on Computer and Communication NCCC'17
http://www.srivasavi.ac.in/ nccc2017@gmail.com

(QoS) links metrics: delay, throughput and signal to interference plus noise ratio (SINR) and returns as output multi-constrained QoS metric used to find the best paths. Next applied to adapt cost functions used to penalize paths previously computed by Dijkstra's algorithm.

This techniques is an central communication technique in the network , Many applications like multicast TV, audio and video conferencing, and multiplayer social gaming use multicast transmission. On the other hand, security in multicast transmissions is crucial, without which the network services are significantly disrupted. Existing secure routing protocols that address different active attacks are still vulnerable due to subtle nature of flaws in protocol design. Moreover, existing secure routing protocols assume that adversarial nodes cannot share an out-of-band communication channel which rules out the possibility of wormhole attack.

Introduction

In sensing data to the base station, wireless sensor networks (WSNs) face some security challenges since such networks impose resource constraints that need to be addressed by the routing mechanism. In surveys, explores, and informs researchers regarding the landscape of multipath routing by providing the motivation behind multipath routing deployment. Subsequently, in this analyzes the security requirements and common attacks in wireless sensor networks. Also, it provides a classification of secure multipath routing protocols on the basis of nature of defense against the WSN attacks. According to the classification, in this investigate the existing secure multipath routing protocols within the WSN domain by discussing their strengths and limitations. A comparative study of the suggested classification is presented based upon the multipath technique, additional security infrastructure, security requirements, corresponding attacks, and efficiency analysis in pursuit of effective secure routing in wireless sensor networks. CMR (Concurrent Multipath Routing) is often taken to mean simultaneous management and utilization of multiple available paths for the transmission of streams of data emanating from an application or multiple applications. In this form, each stream is assigned a separate path, uniquely to the extent supported by the number of paths available. If there are more streams than available paths, some streams will share paths. This provides better utilization of available bandwidth by creating multiple active transmission queues. It also provides a measure of fault tolerance in that, should a path fail, only the traffic assigned to that path is affected, the other paths continuing to serve their stream flows; there is also, ideally, an alternative path immediately available upon which to continue or restart the interrupted stream.

This method provides better transmission performance and fault tolerance by providing:

- Simultaneous, parallel transport over multiple carriers.
- Load balancing over available assets.
- Avoidance of path discovery when reassigning an interrupted stream.

Shortcomings of this method are:

- Some applications may be slower in offering traffic to the transport layer, thus starving paths assigned to them, causing under-utilization.

International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
http://www.ijcsjournal.com Volume 5, Issue 1, No 11, 2017 ISSN: 2348-6600
Reference ID: IJCS-210 PAGE NO: 1312-1316
Sri Vasavi College, Erode Self-Finance Wing 3rd February 2017
National Conference on Computer and Communication NCCC'17
http://www.srivasavi.ac.in/ nccc2017@gmail.com

• Moving to the alternative path will incur a potentially disruptive period during which the connection is re-established.

A more powerful form of CMR (true CMR) goes beyond merely presenting paths to applications to which they can bind. True CMR aggregates all available paths into a single, virtual path. All applications offer their packets to this virtual path, which is de-muxed at the Network Layer, the packets then being distributed to the actual paths via some method such as round-robin or weighted fair queuing. Should a link or relay node fail, thus invalidating one or more paths, succeeding packets are not directed to that (/those) path(s). The stream continues uninterrupted, transparently to the application. This method provides significant performance benefits over the former:

• By continually offering packets to all paths, the paths are more fully utilized.

• No matter how many nodes (and thus paths) fail, so long as at least one path constituting the virtual path is still available, all sessions remain connected. This means that no streams need to be restarted from the beginning and no re-connection penalty is incurred.

It is noted that true CMR can, by its nature, cause out-of-order delivery (OOOD) of packets, which is severely debilitating for standard TCP. Standard TCP, however, has been exhaustively proven to be inappropriate for use in challenged wireless environments and must, in any case, be augmented by a facility, such as a TCP gateway, that is designed to meet the challenge. One such gateway tool is SCPS-TP, which, through its Selective Negative Acknowledgement (SNACK) capability, deals successfully with the OOOD problem.

Another important benefit of true CMR, desperately needed in wireless network communications, is its support for enhanced security. Simply put, for an exchange to be compromised, multiple of the routes it traverses must be compromised.

The new characteristics of Wireless Multimedia Sensor Network (WMSN) and its design issues brought by handling different traffic classes of multimedia content (video streams, audio, and still images) as well as scalar data over the network, make the proposed routing protocols for typical WSNs not directly applicable for WMSNs. Handling real-time multimedia data requires both energy efficiency and QoS assurance in order to ensure efficient utility of different capabilities of sensor resources and correct delivery of collected information. In this Secure Cluster-based Multipath Routing protocol for WMSNs, SCMR, to satisfy the requirements of delivering different data types and support high data rate multimedia traffic. SCMR exploits the hierarchical structure of powerful cluster heads and the optimized multiple paths to support timeliness and reliable high data rate multimedia communication with minimum energy dissipation. Here a light-weight distributed security mechanism of key management in order to secure the communication between sensor nodes and protect the network against different types of attacks. Performance evaluation from simulation results demonstrates a significant performance improvement comparing with existing protocols (which do not even provide any kind of security feature) in terms of average end-to-end delay, network throughput, packet delivery ratio, and energy consumption.

International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
http://www.ijcsjournal.com Volume 5, Issue 1, No 11, 2017 ISSN: 2348-6600
Reference ID: IJCS-210 PAGE NO: 1312-1316
Sri Vasavi College, Erode Self-Finance Wing 3rd February 2017
National Conference on Computer and Communication NCCC'17
http://www.srivasavi.ac.in/ nccc2017@gmail.com

Advantages

•The security mechanisms support and efficiency analysis in secure multipath routing.

•Classification of secure multipath routing based upon the nature of defense.

•Analyze the existing secure multipath routing based upon the classification.

•Provide related figures for each protocol.

•A comprehensive survey with respect to secure multipath routing protocols in all networks.

Security Performance Analysis

In this section examine about the security protection achieved by proposed security scheme against some general security threats in sensor networks, and its performance in terms of memory requirement and scalability:

Defenses from outsider attacks:

Most of the outsider attacks against WMSN routing protocols can be prevented by providing confidentiality (through encryption and authentication) using the shared security keys. Even a simple scheme uses only the shared master key will prevent unauthorized nodes from joining the topology of the network and hence attacks like selective forwarding, acknowledgment spoofing, wormhole, and sinkhole attacks are disallowed. Hello-flood attacks are detected since broadcasting messages in the network done only by using the master key and unique-cluster key. Also by using the unique-node and pair-wise keys, attacks such as Sybil attack is prevented because a single node cannot present multiple identities without having the security keys. The network is also protected against replay attacks as all messages exchanged in the network are tracked by a time stamp and sequence number. Notice that a GM needs only to maintain a one counter for its CH, and a CH needs to keep counters only for its GMs and parents.

Defenses from insider attacks:

Security mechanisms using only the master key cannot protect the network against insider attacks or compromised nodes. Insider attacks can disrupt the network by spoofing or altering routing information, selective forwarding, and broadcasting Hello-floods. Therefore, our proposed security scheme can protect the network against insider attacks by verifying both node identities and bidirectional link, as well as authenticating broadcast messages. Identities can be verified by sharing a symmetric unique-node key for every node with a trusted base station. Two neighboring nodes can authenticate the bidirectional link between them by using the master key to verify other identity and establish a shared pair-wise key for securing the communication between them. Broadcasting can be authenticated by using a unique-cluster key derived from the master key and shared, for example, within a cluster or group of nodes. Using those unique symmetric keys, our security scheme resists against insider attacks and minimizes their effects as a compromised node disturbs only a local part and the rest of the network remains secured.

Scalability:

Our security scheme scales well as it requires only local information for key management without needing of central distribution. Furthermore, the number of security keys needed to be stored at each node does not depend on the network size but only on node density (i.e., average number of group members within a cluster and number of neighboring cluster heads). Average number of

International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
http://www.ijcsjournal.com Volume 5, Issue 1, No 11, 2017 ISSN: 2348-6600
Reference ID: IJCS-210 PAGE NO: 1312-1316
Sri Vasavi College, Erode Self-Finance Wing 3rd February 2017
National Conference on Computer and Communication NCCC'17
http://www.srivasavi.ac.in/ nccc2017@gmail.com

GMs or the size of cluster can be determined by adjusting the value of Thr-High.

Memory requirements:

The majority of nodes (i.e., GMs) need only to store three keys: unique-node, pair-wise, and unique-cluster keys. On the other hand, each CH needs to store the pair-wise keys it shares with its group members and parents, in addition to the unique-node and unique-cluster keys. Recall the powerful capabilities of CHs, storing N keys (N = Ki + Kch + (n + m) × Kij where n is number of parents and m is cluster size), with an average number of parents is 6 (i.e., six different paths) and an average cluster size of 10, does not need considerable memory space

Conclusion

Secure Cluster-based Multipath Routing protocol (SCMR) for WMSNs designed to handle the additional requirements of reliable data delivering of different traffic classes and provide load balancing by using multipath routing. The proposed routing protocol, SCMR, is based on the hierarchical structure of multiple paths established depending on the hop count and received signal strength as an indication on the link quality, delay, and distance between the nodes. SCMR maintains minimum end-to-end delay suitable for real-time and non-real-time data packets to meet their playout deadline, and achieves high throughput and packet delivery ratio by selecting the paths with better link quality and avoiding collisions and interferences. SCMR reduces energy consumption at sensor nodes by moving the multimedia processing complexity as well as the aggregation process to the cluster heads' side along with preventing path loops and path cycles in establishing the routes.