International Journal of Latest Trends in Engineering and Technology
Vol.(9)Issue(1), pp.046-054
DOI: http://dx.doi.org/10.21172/1.91.07
e-ISSN:2278-621X

SECURE KEY DISTRIBUTION WITH SALR USING WIRELESS SENSOR NETWORK

K.Gowrishankar[1] & B. Abirami[2]

Abstract—The major factors that lift the competence of Service Oriented Wireless Sensor Networks are Congestion control and transferring data securely. It is desirable to alter the routing and security outlines adaptively in order to retort effectually to the swiftly fluctuating Network State. Adding complexities to the routing and security schemes increases end to end delay which is not acceptable in service oriented wireless sensor networks. In this project, an innovative proposal of Secure Adaptive Load Balancing Routing (SALR) protocol using data communication has been proposed. SALR adopt the multipath assortment based on Node Strength is done at every hop to decide the most secure and least congested route. The system envisages the unsurpassed direction instead of running the congestion detection and security schemes repeatedly. Simulation results of Delivery Loss Ratio and Packet Delivery Ratio shows that security performance is better than reported protocols and performance of routing path in better results.
Keywords—Wireless Sensor Networks, Secure Adaptive Routing, Load-Balancing, Network Security.

1. INTRODUCTION

Networks of sensors present in Wireless Sensor Network are autonomous and are spatially distributed for capturing data. Sensors have restricted computational and communication power with little memory and limited battery power. The data collected by the individual sensors is then passed on to the base station or the sink. The sink processes the accumulated data for the specific application. Sensor networks have been far and wide applicable in military, environment monitoring, health-care applications and surveillance. In a class of Wireless Sensor Networks, known as the service oriented Wireless Sensor Networks; Sensors have a specific task, and may not be communicating all the time. They trigger communication only when they come across a state change. It is essential to have a technique named "robust routing" that is adaptive to every change in the network along the path of the packet. The resources of a sensor node such as computational power and battery life are limited. Most protocols remain static and could not adapt to the hastily altering state of the network. Both these classes of protocols do not facilitate the efficient functioning of a service oriented Wireless Sensor Networks. In this, every sensor node monitors the load and the strength of each of its neighbors to determine malicious data. It transmits data only to those nodes that are least congested and highly secure. Since the analysis of the two parameters at every hop introduces an overhead in the network we have a feedback system that enables the network to learn from every earlier decision. Routers communicate each other through a routing protocol, broadcasting statistics that empowers them to hand-pick routes between any two nodes on a computer network. A routing protocol shares this information first among immediate neighbors, and then throughout the network. This way, routers gain knowledge of the topology of the network. Wireless sensor networks called are spatially distributed autonomous sensors to monitor physical or environmental conditions, such as temperature, sound, pressure, etc. and to cooperatively pass their data through the network to a main location. The more modern networks are bi-directional, also enabling control of sensor activity. Today such networks are used in many industrial and consumer applications, such as industrial process monitoring and control, machine health monitoring, and so on.

In sensor network, "nodes" from a several hundreds or thousands network, where each nodes are connected to one (or sometimes several) sensors. Each sensor network node has two parts: an internal antenna with radio transceiver or connection to an external antenna, an electronic circuit for interfacing with the sensors, a microcontroller, and an energy source, usually a battery or an embedded form of energy harvesting. A sensor node might vary in size from that of a shoebox down to the size of a grain of dust, although functioning "motes" of genuine microscopic dimensions have yet to be created. The cost of sensor nodes is similarly variable, ranging from a few to hundreds of dollars, depending on the complexity of the individual sensor nodes. Size and cost constraints on sensor nodes result in corresponding constraints on resources such as energy, memory, computational speed and communications bandwidth. The topology of the WSNs can vary from a simple star network to an advanced multi-hop wireless mesh network. The propagation technique between the hops of the network can be routing or flooding. Although there are many types of routing protocols, three major classes are in widespread use on IP networks: Interior gateway protocols type 1, link-state routing protocols, such as OSPF and IS-IS, Interior gateway protocols type 2, distance-vector routing protocols, such as Routing Information Protocol, RIPv2, IGRP.

[1] *Associate Professor, Department of EEE, Rajiv Gandhi College of Engg. & Tech., Pondicherry, INDIA*
[2] Assistant Professor, Department of ECE, Rajiv Gandhi College of Engg. & Tech., Pondicherry, INDIA

A routing protocols used on the web for exchanging routing information between Autonomous Systems. Many routing protocols are defined in documents called RFCs. Some versions of the Open System Interconnection(OSI) networking model distinguish routing protocols in a special sub layer of the Network Layer(Layer 3).The specific characteristics of routing protocols include the manner in which they avoid routing they require to reach routing convergence, their scalability, and other factors.

1.1 Interior Gateway Protocol

Interior gateway protocols uses exchange of routing information using a single routing domain. Examples of IGPs include:

- Open Shortest Path First(OSPF)
- Routing Information Protocol(RIP)
- Intermediate System to Intermediate System(IS-IS)

1.2 Exterior Gateway Protocol

Exterior gateway protocols uses exchange of routing information between two or more autonomous systems. Examples include:

- Exterior gateway protocol (EGP)
- Border gateway protocol (BGP)

1.3 Routing Software

Several software implementations exist for the common routing protocols are listed below. Examples of open-source applications are Bird Internet routing daemon, Quagga, GNU Zebra, Open BGPD, Open OSPFD, and XORP.

1.4 Routed Protocol

Few certification courses in a network distinguish between routing and routed protocols. A routed protocol, deliver application traffic and provides appropriate addressing information (Network Layer) and also addressing to allow a packet to be forwarded from one network to another.

2. BACKGROUND

The existing work in WSNs, is multipath routing schemes which demonstrated the effectiveness of traffic distribution over multipath to fulfill the quality of service requirements of applications. However, the failure of links might significantly affect the transmission performance, scalability, reliability, and security of WSNs. Considering the reliability, congestion control, and security for multipath, it is desirable to design a reliable and service-driven routing scheme to provide efficient and failure-tolerant routing scheme. In this paper, an evaluation metric, path vacant ratio, is proposed to evaluate and then find a set of link-disjoint paths from all available paths.

A congestion control and load-balancing algorithm that can adaptively adjust the load over multipath is proposed. A threshold sharing algorithm is applied to split the packets into multiple segments that will be delivered via multipath to the destination depending on the path vacant ratio.

The Wireless Sensor Networks (WSNs) have the potential for many applications to revolutionize the way to acquire information and interact with the physical world. Unfortunately, most existing WSNs are designed for specific purposes and lack of standard operations and representation for sensor data that can be used by upper layer applications or services. Recently, service-oriented architectures for WSNs have been proposed to support the interoperability between different applications where the functionalities provided by WSNs are treated as services, e.g., data aggregation service, data processing service, and localization service

In service-oriented applications, services with various performance metrics, e.g., bandwidth, delay, load balancing, and reliability, have been well studied within the service systems where each node provides the quality-of-service (QoS) parameters associated with these services. In a service-oriented WSN, applications can be designed over service requirements to depart from current application-specific or generic WSNs.

A large volume of traffic is exchanged over WSNs; as a result, how to improve the throughput of WSNs is a critical challenge in the design of service-oriented WSNs. It is desirable to design an adaptive multipath routing scheme that is able to significantly reduce the downstream traffic and dynamically support QoS requirements, as well as achieve reliable paths from a source node to a destination node. Each node on a path should be able to evaluate the performance of its next-hop neighbors according to the reliability of the path. The routing scheme should provide the services with bandwidth guaranteed multipath, which help these services be run over secure and reliable network architecture. Most existing multipath routing protocols generally do not exploit the service-oriented architecture over WSNs. Link-disjoint-based multipath routing is a good idea to treat each application as a service task that can be supported via more flexible protocol design and resource management. The service oriented WSNs should avoid forwarding routing messages to unrelated nodes. Each node should be able to detect

service related nodes and forward to them the routing message. In this, a multipath routing scheme is proposed, which features the following:

1) Application independence
2) Secure data delivery
3) Adaptive congestion control and rate adjustment
4) Extensibility.

3. LITERATURE SURVEY

All The system called Cyber-physical-social system (CPSS) allows individuals to share personal information collected from not only cyberspace but also physical space. This has resulted in generating numerous data at a user's local storage. However, it is very expensive for users to store large data sets, and it also causes problems in data management [1]. Therefore, it is of critical importance to outsource the data to cloud servers, which provides users an easy, cost-effective, and flexible way to manage data, whereas users lose control on their data once outsourcing their data to cloud servers, which poses challenges on integrity of outsourced data. An auditor needs to manage user's certificates to choose the correct public keys for verification.

Here, a secure certificate less public integrity verification scheme (SCLPV). The SCLPV is the first work that simultaneously supports certificate less public verification and resistance against malicious auditors to verify the integrity of outsourced data in CPSS. In comparison with the best of integrity verification scheme Achieving resistance against malicious auditors, the communication cost between the auditor and the cloud server of the SCLPV is independent of the size of the processed data, meanwhile, the auditor in the SCLPV does not need to manage certificates.

In wireless sensor networks, the secure end-to-end data communication is needed to collect data from source to destination. Collected data are transmitted in a path consisting of connected links. All existing end-to-end routing protocols propose solutions in which each link uses a pair wise shared key to protect data. This paper provides a novel design of secure end-to-end data communication. A newly published group key pre-distribution scheme in our design, such that there is a unique group key, called path key, to protect data transmitted in the entire routing path [2]. Specifically, instead of using multiple pair wise shared keys to repeatedly perform encryption and decryption over every link, our proposed scheme uses a unique end-to-end path key to protect data transmitted over the path. Our protocol can authenticate sensors to establish the path and to establish the path key. The main advantage using this protocol is to reduce the time needed to process data by intermediate sensors. Moreover, our proposed authentication scheme has complexity O (n), where n is the number of sensors in a communication path, which is different from all existing authentication schemes which are one-to-one authentications with complexity O (n2). The security of the protocol is computationally secure.

In this paper, an office climate monitoring and control system is designed and implemented. The system consists of various wireless sensor nodes and a control node. The sensor nodes provide the sensor data necessary to determine occupancy and the control node executes the algorithm which decides whether to activate cooling or heating based on the sensor data. Conventional High Voltage Advance Computing systems usually achieve the desired control level by means of simple on-off control which can often result in high energy wastage. A potential solution to this issue is intelligent self-regulating High Voltage Advance Computing controllers which base their actions/decisions on sensor data [3]. This system can serve as a controller and can be integrated into High Voltage Advance Computing systems in smart buildings. It is shown that the developed control algorithm executed on the control node results in an improvement of up to 39% in energy efficiency over conventional on-off controllers for High Voltage Advance Computing systems.

Later, Wireless Sensor-Actor Networks (WSANs), actors collect sensor readings and respond collaboratively to achieve an application mission. Since actors coordinate their operation, a strongly connected network topology would be required at all time. In addition, the path between actors may have to be capped in order to meet latency constraints. However, a failure of an actor may cause the network to partition into disjoint blocks and would thus violate such connectivity goal. One of the effective recovery methodologies is to autonomously reposition a subset of the actor nodes to restore connectivity [4].

Contemporary schemes rely on maintaining 1 or 2-hop neighbor lists an predetermine criteria for node's involvement in the recovery. However, 1-hop based schemes often impose high node relocation overhead. In addition, the repaired inter-actor topology using 2-hop schemes often differs significantly from its pre-failure status and some. Inter-actor data paths may get extended. This paper presents a Least-Disruptive topology Repair (LeDiR) algorithm. LeDiR relies on the local view of a node about the network in order to devise a recovery plan that relocates the least number of nodes and ensures that no path between any pair of nodes is extended. LeDiR is localized and distributed algorithms that leverages existing path discovery activities and imposes no additional pre figure communication overhead.

The Wireless charging is a promising way to power wireless nodes' transmissions. This paper considers new dual function access points (APs) which are able to support the energy/information transmission to/from wireless nodes. We focus on a large-scale wireless powered communication network (WPCN), and use stochastic geometry to analyze the wireless nodes' performance tradeoff between energy harvesting and information transmission. We study two cases with battery-free and battery-deployed wireless nodes. For both cases, we consider a harvest-then-transmit protocol by partitioning each time frame into a downlink (DL) phase for energy transfer, and an uplink (UL) phase for information transfer. By jointly optimizing frame partition between the two phases and the wireless nodes' transmit power; we maximize the wireless nodes' spatial throughput subject to a successful information transmission probability [5].

For the battery-free case, we show that the wireless nodes prefer to choose small transmit power to obtain large transmission opportunity. For the battery-deployed case, we first study an ideal infinite-capacity battery scenario for wireless nodes, and show that the optimal charging design is not unique, due to the sufficient energy stored in the battery. We then extend to the practical finite-capacity battery scenario. Although the exact performance is difficult to be obtained analytically, it is shown to be upper and lower bounded by those in the infinite capacity battery scenario and the battery-free case, respectively.

4. PROPOSED WORK

In proposed system the secure adaptive load balancing routing protocol. It can be divided into three parts. They are Adaptive load balancing; Security based on Node Strength Route prediction based on learning from previously chosen routes.

4.1 Congestion Detection

Our approach to solving the congestion problem is differ from the conventional one is

- To prevent congestion from taking place.
- Rather than redistributing the load after a congestion has taken place.
- Our load balancing scheme is such that each and every node in the network is continuously.
- Monitored for congestion.

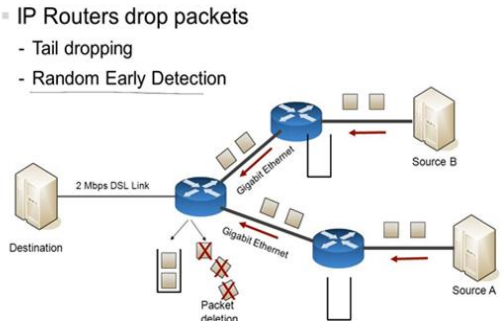

Figure 1: Congestion Detection

When the system feels that a particular node is going to be congested in the near future, then a dynamic load balancing scheme is incorporated to prevent that node from entering into a congestion state. The congestion detection algorithm basically classifies anode as Tending towards Congestion [TTC] or Available. A node is classified as TTC if its buffer can at-most accommodate only one packet sent by each of its neighbor. Proposed method maintains information about its buffer capacity and the current number of packets in its buffer. Once it realizes that it is tending towards congestion, it immediately sends out a message to all its neighbors updating them about its status. A node which sends such a message must also send an available message to all its neighbors as soon as it comes out of the TTC situation.

4.2 Node Strength

Here, the nodes that clear the congestion detection test are checked for node strength. The node strength of node is the capability of that node to detect malicious data.

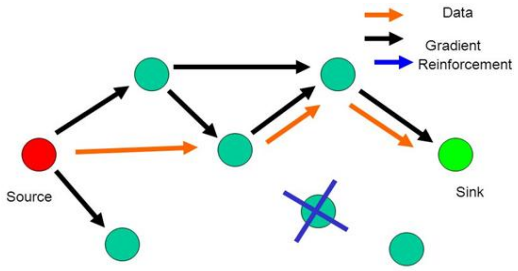

Figure 2: Direct Diffusion

To determine the node strength of a particular node, we need to obtain the total number of true key matches and the total number of false key matches of that node. A node with the highest node strength among other nodes is chosen to route the packet.

4.3 Packet Routing

Once the node with the highest node strength is selected, it is certain that the node is least congested as well. At the next node, the entire dynamic secure route selection procedure is executed to determine the next hop for the packet. The path may not remain uncongested or secure forever. Therefore we cannot rely on the same path throughout the transmission.

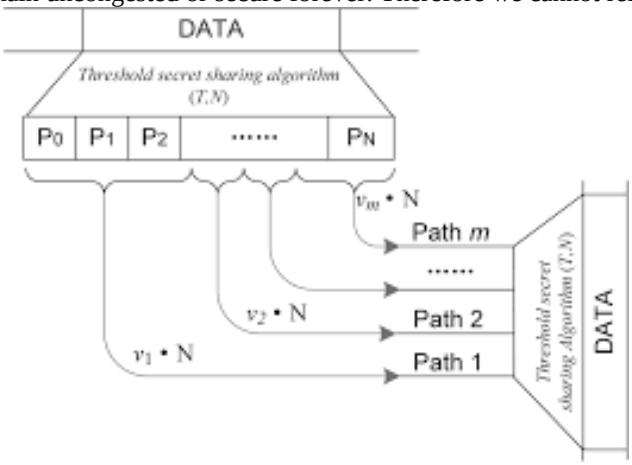

Figure 3: Secret key sharing

4.5 Route Prediction

The computational overhead leveraged on the network because of dynamic load balancing and secure route selection based on node strength is significant. In order to make sure that this does not impact the end-to-end delay of the transmission of data, the system continuously learns from previous routing decision. The routing decision is based on node strength of each and every node by applying congestion detection with the help of trust factor, that is a key matching technique determine by the number of true key matches and false key matches. The true key is directly proportional to the node strength of a node and the false key is indirectly proportional to the node strength of a node, it seems that it is not an adjacent node which involves in the particular data transmission process.This significantly reduces the time required for determining the route based on Route statistics collection.

4.6 Route Statistics Collection

Proper prediction requires a good amount of training data to support it. The collection of the training data to make a reliable prediction in future.

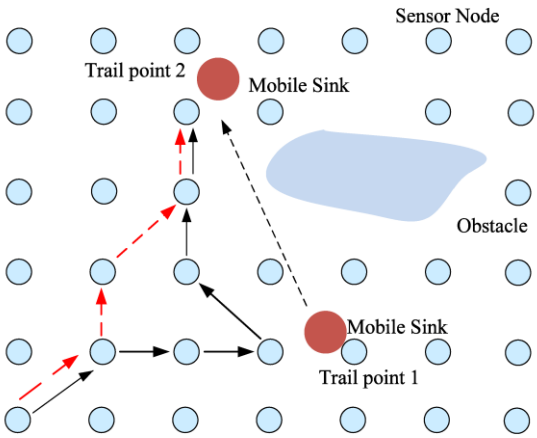

Figure 4: Route prediction

Algorithm for SALR protocol

- Weight assignment

- Algorithm for weight assignment
- Prediction and feedback

Algorithm: Secure Adaptive Load-Balancing Routing
Phase 1: Congestion Detection
Input: available Multipath
Output: PNL
begin
if by Pass == FALSE then
PNL ← available Multipath
if CONGEST node == TRUE then
PNL ← PNL − node
else if AV AILABLE node == TRUE then
PNL ← PNL + node
else
goto Phase 3
end
Phase 2: Node Strength
Input: PNL
Output: SN
begin
if by Pass == FALSE then
for PN in PNL do
NS ← get NS(PN)
SNL ← append({PN,NS})
SN ← get Maximum NS(SNL)
else
Transmit the packet
end
Phase 3: Constructing the LT
Input: path i
begin
if path i in LT then
ni ← ni +1
delay i ← delay i + delay rec
update LT (path i, delay i)
else
ni ← 1
delay i ← delay rec
insert LT (path i, delay i)
end
Phase 4: Weight Adjustment
Input: ni, delay i
begin
Avg Delay i ← delay i
ni
rn ← ni
nt
rAvg Delay ← Avg Delay i
Avg Delay t
Wi ← rn
rAvg Delay
update LT (path i,Wi)
end
Phase 5: Prediction
Input: LT
begin

pj ← get Route With Max Weigh t(weight pi)
by Pass ← TRUE
packet ← append(pj, timestamp)
neighbour ← get Next Node(pj)
send(packet,neighbour)
if node i == dest then
ack ← append(pi, delay)
send(ack, source)
goto Phase 1
end

4.7 Weight Assignment

Once the threshold number of packets have been transmitted, i.e., once sufficient training data is collected, each of thethe routes is analyzed and weights are assigned to them.The weight of a route is the trust factor of that route. The weight of each route is compared to determine the best route for a prediction. A route is trust worthy if it has lower delay and a good number of packets have been sent along that route.

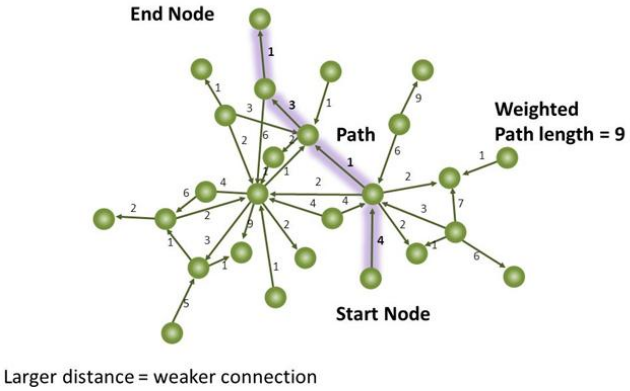

Figure 5: Weight assignment

4.8 Prediction And Feedback

This is the final phase in which the system predicts an appropriate route for transmission of the packet. The weights of each route reflect the trust factor of that route. The route with highest weight is the one that has lower delay and has transmitted a good number of packets compared to other routes. Such a path which is trustworthy is then chosen to route the next packet.

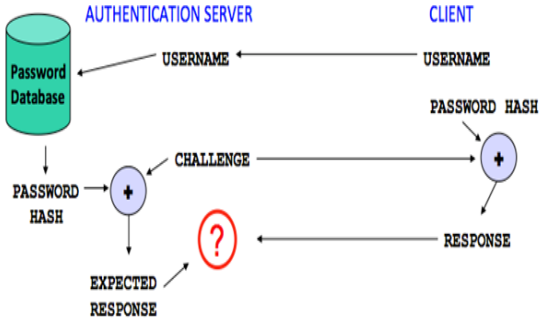

Figure 6: Security maintaining

5. RESULT

The Evaluate the efficiency of our scheme based on the data loss ratio, the packet delivery ratio, the average delay, and compare these results with SM-AODV, a similar multipath dynamic routing scheme. Our algorithm is implemented using the discrete event network simulator NS-2.35. The area of node deployment is 1000m*1000m with the base station positioned close to the origin. The remaining nodes are deployed randomly. The base station is placed at the bottom left corner of the deployment area, so that it is outside the danger zone.

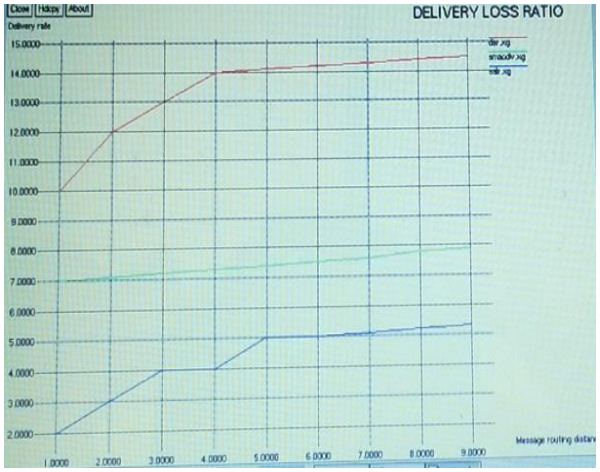

Figure 7: Data loss ratio against Different number of Paths

Hence, in case any accidents occur in the deployment site the base station is not affected. The simulation parameters are given in Table. The number of sensor nodes is varied from 100 to 150 and simulation runs are carried out for duration 100 seconds. It is assumed that the network topology is known and multi paths can be found in each source destination pair which is at least three hops. In this simulation and performance analysis, we have to compare two techniques. They are Secure and Adaptive Load Balancing Routing Protocol (SALR) and Secure Mode Ad-hoc Distance Vector(SM-AODV).Data loss ratio is a metric which can illustrate the dynamic adaptability of the congestion control scheme of SALR. Figure 7 shows the data loss ratio with different paths for SM- AODV and SALR, where a fixed data stream is generated with Constant Bit Rate (CBR). SALR protocol shows an improvement in data loss ratio of up to 62.5% when compared with SM-AODV. When the number of paths is less, the data loss ratios of both SALR and SM-AODV are quite close.However, an increase in the number of paths has an adverse effect on the performance of SM-AODV while the SALR protocol is much more stable. This is mainly because of our dynamic load balancing scheme which determines if a node is tending towards Congestion [TTC].

Figure 8: Packet Delivery Ratio against Mobility of Nodes

Figure 8 shows an improvement in the packet delivery ratio of about 6% is achieved when compared to SM-AODV. Initially, at lower levels of node mobility not much difference is observed in the performance of SALR and SMAODV. But as the mobility in the network increases, SALR achieves a considerable degree of improvement in successfully delivering packets to the destination. This is a direct consequence of our Node Strength phase which determines the most secure node based on the node's ability to detect malicious data. This increases the overall reliability of the network, which helps in establishing trustworthiness of the sensor network which is extremely essential in real applications.

6. CONCLUSION

This paper successfully incorporate all the features mentioned, to a prototype model "secure key distribution with SALR using wireless sensor network". A special kind of Wireless Sensor Network which is service oriented wireless sensor network is used in which real time reliable data delivery is a major requirement. In Secure and Adaptive Load-Balancing Routing protocol caters to such requirements by adopting a learning based dynamic load balancing model with advanced security. The

algorithm employs a hop-by-hop mechanism; each intermediate node determines the least congested neighbor which has the highest node strength before forwarding a packet to it. Performing both congestion detection and security analysis to each and individual hop can result in increased delay and energy consumption. To overcome this feedback mechanism is employed in which the source keeps track of the entire available multipath and their corresponding delays. We achieve considerable improvement in average deferral, delivery ratio of the packets and data loss ratio when compared to Secure Mode Ad-hoc Distance Vector (SM-AODV) by incurring a little memory overhead while collecting training data. Further, the feedback is continued even subsequently the source chooses a path with the aim of adapt to any future changes in the network characteristics. We technologically advanced a mathematical model to detect congestion and to measure node strength and trust factor. Future work would involve determining an exact threshold point for commencing the prediction phase which would provide a balanced trade-off between delays and secure it.

7. REFERENCES

[1] Yuvan Zhang, Shui Yu, Chunxiang Xi, Hongwei li, Xiaojun Zhang. Secure Certificate less Public Verification for Cloud-based Cyber Physical-Social Systems against Malicious auditors. IEEE Transactions on Computational Social Systems, Vol.2, No. 4(Dec 2015), pp.: 150-170.

[2] Timothy W. Foster, Deep Vardhan Bhatt, Gerhard P. Hancke, Bruno Silva. Web-based office climate control system using Wireless sensors. IEEE Sensors Journal, Vol. 16, No. 15(Aug 2016), pp.: 6101-0113.

[3] A. Abbassi, M. Younis, U. Baroudi. Restoring connectivity in wireless sensor-actor networks with minimal topology changes. IEEE International Conference on Communications (ICC-10), South Africa, 23-27 May 2010, pp.: 1-5.

[4] Yue ling che, Ruizang. Spatial Throughput Maximization of Wireless Powered Communication Networks. IEEE Sensors Journal 2015.

[5] A. Selcuk Uluagac, Raheem A. Beyah, John. A. Copeland. Secure Source-Based Loose Synchronization (SOBAS) for Wireless Sensor Networks. IEEE Transactions on Parallel and Distributed Systems, Vol. 24, No. 4 (April 2013), pp. 803-813.

[6] Ameer A. Abbasi, Mohammed F. Younis, Uthman. A. Baroudi. Recovering From a Node Failure in Wireless Sensor-Actor Networks with Minimal Topology Changes. IEEE Transactions on Vehicular Technology, Vol. 62, No. 1 (Jan 2013), pp. 256-27.

[7] Tao Shu, Marwan Krunz, Sisi Liu. Secure Data Collection in Wireless Sensor Networks Using Randomized Dispersive Routes. IEEE Transactions on Mobile Computing, Vol. 9, No. 7 (July 2010), pp. 941-954.

[8] Guoxing Zhan, Weisong Shi, Julia Deng. Design and Implementation of TARF: A Trust-Aware Routing Framework for WSNs. IEEE Transactions on Dependable and Secure Computing, Vol. 9, No. 2 (2012), pp.184-197.