International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 08 Issue: 06 | June 2021 www.irjet.net p-ISSN: 2395-0072

Secure Data Re-Routing Using SDN

Mohith K J[1], C K Vanamala[2]

[1]*PG Student, Dept. of Information Science and Engineering, NIE, Mysore, Karnataka, India*
[2]*Associate Professor, Dept. of Information Science and Engineering, NIE, Mysore, Karnataka, India*

Abstract – *An SDN [Software Defined Network] is connecting with in light of the fact that it gives versatile and dynamic coordinating by detaching control and data planes. It has an overall view on network topography in light of its joined control and is in this manner by and large applied to traffic planning, interface frustration recovery, and weight changing. As an association expands, the repeat of stream invigorates, where a lot of streams ought to be moved to new courses, similarly increases. During stream update, capability and consistency are two essential troubles. Capability suggests how fast a lot of given stream revives are done, while consistency implies evasion of blackholes, circles, network blockages, and gridlocks during invigorates. Sans blackhole infers that there is no theoretical stream inciting a stalemate. Circle free suggests that there is no temporary indirect course in the association. Obstruct free strategies the measure of transfers on an association should not outperform its association limit. Since a SDN can deal with its update demand, it is depended upon to keep up these properties by calculating a sensible update plan. In this paper SDN, it detaches control plane programming and data plane gear. As, one controller can screen and manage different switches or switches. Association devices thusly simply need to propel packs. The controller is executed by unadulterated programming and orders data planes by shows like OpenFlow. Accordingly, new correspondence shows can be even more easily recognized with little hardware impediment. Along these lines, SDN can save gear upgrade costs and change in accordance with genuinely growing programming needs.*

***Key Words*: SDN, Sink opening assault, Network layer, LA-ASD,**

1. INTRODUCTION

An association configuration can be isolated into control plane, data plane, and the load up plane. Data plane advances groups by investigating stream tables. Control plane masterminds and updates stream tables for data plane. The load up plane is at risk for noticing and planning association gadgets. SDN is connecting with because it gives versatile and dynamic coordinating by disconnecting control and data planes. It has an overall view on network geology due to its joined control and is in this manner for the most part applied to traffic planning, interface frustration recovery, and weight changing. As an association expands, the repeat of stream invigorates, where a lot of streams ought to be moved to new courses, similarly increases. During stream update, capability and consistency are two central challenges. Capability implies how speedy a lot of given stream revives are done, while consistency insinuates evasion of blackholes, circles, network blockages, and gridlocks during invigorates. Sans blackhole infers that there is no speculative stream inciting a stalemate. Circle free suggests that there is no temporary indirect course in the association. Obstruct free strategies the measure of transfers on an association should not outperform its association limit. Since a SDN can deal with its update demand, it is depended upon to keep up these properties by calculating a sensible update plan.

2. Protocol stack of SDN

Before profound making a plunge research one ought to have the information working of remote sensor organization. Following is the engineering of remote sensor organization

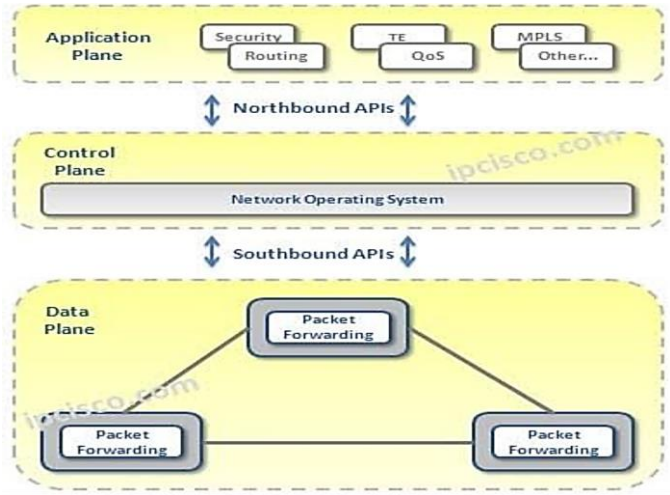


Fig 1: SDN Architecture

In a proposed framework, I attempted to carry out a powerful calculation for stream update in a SDN by thinking about both consistency and effectiveness. It contains four stages. In the primary stage, each stream to be refreshed is divided into various portions, if conceivable, to expand update parallelism. In the subsequent stage, we produce a worldwide reliance chart from these stream sections to build a worldwide view. In the third stage, we begin to refresh rules of stream fragments and change the reliance diagram powerfully for productivity while keeping up network consistency. In the

last stage, we handle those halts that are not yet settled in the third stage.

2.1 Security Requirements for sinkhole detection network

- Confidentiality
- Integrity
- Availability
- Authentication and approval
- Non-Repudiation
- Freshness

2.2 Layer Wise attacks

Table -1: Attack in SDN

S. No	Layer	Attacks
1.	Physical	Jamming and Tampering
2.	Data Link	Collision Unfairness Exhaustion
3.	Network	Sinkhole Wormhole Sybil Selective Forwarding Hello Flood
4.	Transport	Flooding Desynchronization
5.	Application	Cloning Denial-of-service

3. Sinkhole Attack

In a sinkhole assault interloper catches a genuine hub and update its steering data that it is one jump away or briefest separation from base station to draw in all neighbor traffic.

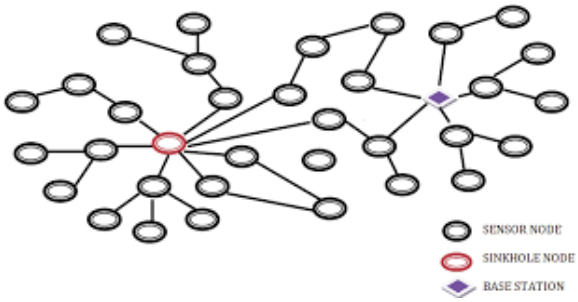
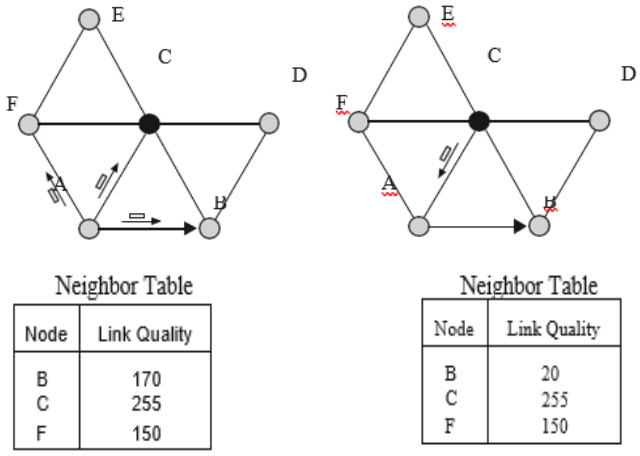


Fig -2: Sink hole attack

When intruder achieve this, it will launch a sinkhole attack. Sinkhole attack is an insider attack. Because of many to one communication nature of WSN where every node wants to send the information to base station, makes WSN vulnerable to sinkhole attack. Below we have presented an example of sinkhole attack in Mint-route protocol.



(A) (B)

Fig -3: Example of sinkhole attack

Mint-Route convention is a sort of convention which is generally utilized in remote sensor organization. It was planned intentionally for the remote sensor organization, it is light and reasonable for sensor hubs which have least stockpiling limit, low calculation force and restricted force supply. Mint Route convention utilizes connect quality as a measurement to pick the best course to send parcel to the Base Station (Krontiris et al [10]). From above figure (a) when c launcher sinkhole figure, it will show its connection quality with greatest worth of 255. Still hub A won't change its parent hub to C from B. So according to figure (b)node C will send new course update packer that hub B's connection quality worth falls up to 20 and hub C will mimic hub B so hub A will accept that bundle came from hub B and hub A will change its parent hub from B to C.

3.1 Difficulties in Detection of Sinkhole Attack:

1. Broadcast Nature of Communication (Many to one)
2. Attack is eccentric
3. Insider Attack
4. Limited assets and Unique Properties
5. Physical Capturing

3.2 Calculations Used in The Project

LA-ASD

LA-ASD is an idea that falls under Unsupervised Learning. This arrangement of rules might be utilized to find offices internal unlabeled insights.

- Step1: Making the Data Frame for two-dimensional dataset of the understudies who have taken tests on a particular course
- Step2:

  Discovering the centroids dependent on the linearization obviously based semantic

In the code, you can determine the kind of groups. For the present circumstance, dole out 3 groups as follows:

LA-ASD(n_clusters=3). fit(df)

- Step3:

  Haphazardly allot each measurement thing to a group: Assignment arbitrary focuses to a bunches to register group centroids: The centroid of records components are figure utilizing distance method

- Step4:

  Re-dole out each highlight the closest group centroid dependent on the course and the clients' hubs.

  Re-register group centroids, presently re-figuring the centroids for the bunches.

- Step5:

  Rehash stages 4 and 5 till no redesigns are reasonable: Similarly, we'll rehash the fourth and fifth steps till we'll acquire worldwide optima.

  When there can be no further exchanging of records factors among bunches for progressive rehashes. It will check the end of the arrangement of pointers if not expressly referenced.

4. Literature Survey

Prakash C Kala, Arun Prakash Agrawal, Rishi Rajan Sharma at [5] introduced a novel procedure to recognize sinkhole assault. In that when throughput decreased than anticipated throughput, sensor hub requests the interesting key of base station. Base station figure key with Armstrong number. So vindictive hub which parodies the ID of base station can not give the extraordinary key and identified as malevolent hub.

Mohammad Wazid1, Ashok Kumar Das, Saru Kumari and Muhammad Khurram Khan at [6] proposed method to recognize sinkhole in progressive organization utilizing LEACH convention. In that they proposed 2 calculations in which they distinguish suspected hub utilizing sinkhole hub presence calculation and characterize suspected hub type as SMD (sinkhole message adjustment hub), SDP (sinkhole message dropping hub) and SDL (sinkhole message defer hub) by utilizing sinkhole hub recognizable proof calculation.

N. Mohammaed Yasin N. Balaji G. Sambasivam M. S. Saleem Basha P. Sujatha at [7] introduced a jump check observing strategy to distinguish sinkhole assault. This procedure distinguishes assault with precision with 96% and applied to directing convention that keeps up progressively a bounce check boundary.

Arya I s and Dr. Bingu g s at [8] propose a cross layer approach for recognition of sinkhole assault utilizing versatile specialist. The recognition rate is expanded as they distinguish influenced group rather than influenced hub. Course was taken out when it was gotten to more much of the time than anticipated to. For correlation they utilized re-bunching technique with versatile specialist strategy as far as energy utilization and leftover energy. Result demonstrates portable specialist method more productive than re-grouping.

Krontiris, I., Dimitriou, T., Giannetsos, T. what's more, Mpasoukos, M.at [9] proposed a standard based strategy to distinguish sinkhole assault. They introduced 2 principles "for every overhead course update bundle the ID of the sender should be diverse your hub ID" and "for every overhead course update parcel the ID of the sender should be one of the hub ID in your neighbors". These 2 standards carried out in interruption identification procedure. At the point when any hub disregards any of the standard than IDS will trigger an alert yet cannot give ID of the malignant hub.

Again Krontiris, I., Giannetsos, T. furthermore, Dimitriou, T. at [10] utilized same guideline-based procedure. In which they characterize 2 standards ""rule for every overhead course update parcel the ID of the sender should be one of hub ID in your neighbors" and "for each pair of parent and youngster hub their connection quality they promote for the connection between them, the distinction can't surpass 50."

Roy, D.S., Singh, A.S. also, Choudhury, S. at [11] proposed a powerful trust-based procedure in which each hub ascertains trust of their neighbor hub dependent on experience of connection and send the data to the base station. Then, at that point dependent on the trust data base station chooses which hub is sinkhole hub. Hence, the trust esteem falls underneath typical worth 0.5 for the hub will be considered as sinkhole hub.

Coppolino, L., D'Antonio, S., Romano, L., and Spagnuolo, G. at [12] proposed a half and half-based interruption discovery procedure joining both abnormality based and rule-based method. In this half breed interruption recognition was connected to each sensor hub and shared their assets. The dubious hubs put into boycott and this data ship off focal specialist for ultimate conclusion. This method was intended for static organization.

Sharmila, S., and Umamaheswari, G.at [13] proposed a method utilizing message digest calculation to distinguish sinkhole assault. In that when an interloper hub mask itself to nearest to base station by publicizing counterfeit steering data the sender hub.

Md. Ibrahim Abdullah, Mohammad Muntasir Rahman and Mukul Chandra Roy at [14] proposed a jump include based procedure in which at a respectable starting point station initially sends hi bundles to develop neighbor information base which contains nod_id of neighbor and bounce check esteem. Hub compute normal bounce tally esteem barring most minimal jump tally esteem and nod_id. Then, at that point contrasts normal jump distance and most reduced bounce distance in the event that it is more prominent than edge that mark it as dubious.

5. Proposed Design

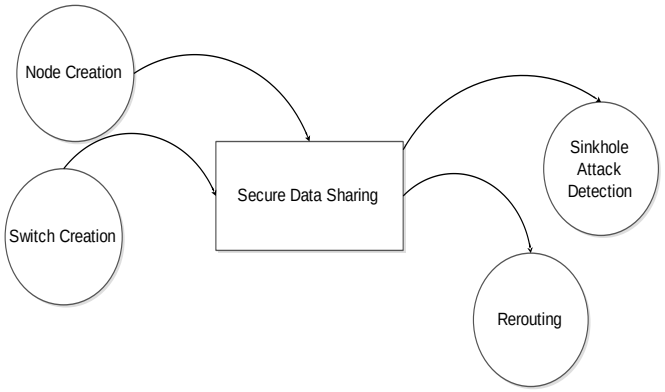


Fig -4: design implementation

In this section we emphases on the overall system operations. For every request from the user there will be an response from the server. Firstly, user should register to application. The server will store the data to database. Then the user will enter their credentials to login. this data will be validated with the database for unauthorized access. Now the user will upload the file to network and it is stored in database. the uploaded file will convert into data packets for transmission. the nodes count is given to create user defined nodes and it is same for switches count. now comes the phase for switches and node mapping which is done by server-side programming. from the user request is generated. sever will detect if there is any sinkhole attack occurs. If found server will re-route from sinkhole node to another node for normal transmission of data to the destination.

6. Result analysis

A large portion of the traditional and SDN-put together organization frameworks are based with respect to devoted and amazing stages. To think about the exhibition of ordinary and SDN-based organization frameworks, and between the two SDN structures portrayed above, we carried out network frameworks on a basic PC stage, under the presumption that contrasts between basic stage exhibitions demonstrate the distinctions in execution of committed organization frameworks stages. We verified this presumption by testing the distinctions in execution utilizing an amazing organization processor-based-stage notwithstanding the basic PC stage. fig shows how the sinkhole attack occurs in network and re-routing process is done by nodes.

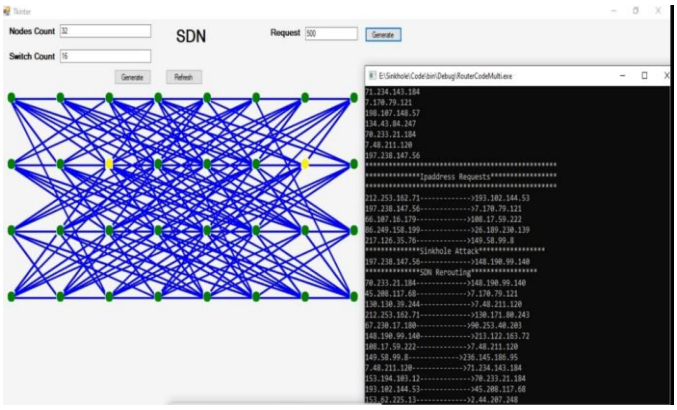


Fig -5: Stimulation of SDN

7. CONCLUSIONS

In this venture, I propose another segment reliant upon data rerouting, which intensely develops strong secure-orchestrated coordinating routes in SDN, and aggregates switch center point limits. The structure takes the center points' association and security limits as fundamental estimations, in this manner ensuring the establishment of a strong coordinating way and carrying out malevolent traffic discovery, Isolation, and information rerouting configuration.

In the future, framework can be improved to distinguish a lot more assaults on the web and to erase the pernicious hub. Further exploration can be made to improve the exactness and effective of the proposed framework

REFERENCES

[1] Furrakh Shahzad, Maruf Pasha, Arslan Ahmad "A Survey ofActive Attacks on Wireless Sensor Networks and theirCountermeasures" International Journal of Computer Science and Information Security (IJCSIS), Vol. 14, No. 12, December 2016

[2] George W. Kibirige, Camilius Sanga "A Survey on Detection of Sinkhole Attack in Wireless Sensor Network" (IJCSIS) International Journal of Computer Science and Information Security, Vol.13, No. 5, May 2

[3] S. Nithya, Dr.C. Gomathy "A Survey of Attacks in wireless Sensor Network" International Journal of Applied Engineering Research, ISSN 0973-4562 Vol. 10 No.26 (2015)

[4] S. Nithya, K.VijayaLakshmi , V.PadmaPriya "A Review of Network Layer Attacks and Countermeasures in WSN" IOSR Journal of Electronics and Communication Engineering (IOSR-JECE) e-ISSN: 2278-2834, p- ISSN: 2278-8735.Volume 10,Issue 6,Ver. I (Nov - Dec .2015)

[5] Prakash C Kala, Arun Prakash Agrawal, Rishi Rajan Sharma "A Novel Approach for Isolation of Sinkhole Attack in Wireless Sensor networks" 10th International Conference on Cloud Computing, Data Science & Engineering (Confluence).

[6] Mohammad Wazid1, Ashok Kumar Das, Saru Kumari

and Muhammad Khurram Khan "Design of sinkhole node detection mechanism for hierarchical wireless sensor networks" SECURITY AND COMMUNICATION NETWORKS Security Comm. Networks 2016; 9:4596–4614 Published online 17 October 2016 in Wiley Online Library(wileyonlinelibrary.com). DOI:10.1002/sec1652

[7] N. Mohammaed Yasin N. Balaji G. Sambasivam M. S. Saleem Basha P. Sujatha "ADSMS: ANOMALY DETECTION SCHEME FOR MITIGATING SINK HOLE ATTACK IN WIRELESS SENSOR NETWORK" International Conference on Technical Advancements in Computers and Communications 2017 IEEE

[8] ARYA I S, Dr. BINU G S "Cross Layer Approach for Detection and Prevention of Sinkhole Attack Using A Mobile Agent" Proceedings of the 2nd International Conference on Communication and Electronics Systems (ICCES 2017) IEEE Xplore Compliant.

[9] Krontiris, I., Dimitriou,T., Giannetsos,T. and Mpasoukos,
M. (2008). Intrusion Detection Sinkhole Attacks in Wireless Sensor Network. LNCS 4837, pp. 150-161.

[10] Krontiris, I., Giannetsos, T. and Dimitriou, T. (2008). Launch Sinkhole Attack in Wireless Sensor Network; the Intruder Side.

[11] Coppolino, L., D'Antonio, S., Romano, L., and Spagnuolo,G. (2010). An intrusion detection system for critical information infrastructures using WSN technologies.

[12] Roy, D.S., Singh, A.S. and Choudhury, S. (2008). Countering Sinkhole and Blackhole Attacks on Sensor Networks using Dynamic Trust Management

[13] Sharmila, S., & Umamaheswari, G. "Detection of Sinkhole Attack in Wireless Sensor Networks Using Message Digest Algorithms" 2011 International Conference on Process Automation, Control and Computing, IEEE.

[14] Md. Ibrahim Abdullah, Mohammad Muntasir Rahman and Mukul Chandra Roy "Detecting Sinkhole Attacks in Wireless Sensor Network using Hop Count" I.J. Computer Network and Information Security, 2015 MECS.

[15] Imandi Raju and Pritee Parwekar "Detection of Sinkhole Attack in Wireless Sensor Network".

[16] Krontiris, I. Dimitrou, T. Freiling, F.C. (2007). Towards intrusion detection in wireless sensor networks. Proceedings of the 13th European Wireless Conference, Paris, France, April 2007.

[17] Coppolino, L., D'Antonio, S., Romano, L., and Spagnuolo,G. (2010). An intrusion detection system for critical information infrastructures using WSN technologies.

[18] Roy, D.S., Singh, A.S. and Choudhury, S. (2008). Countering Sinkhole and Blackhole Attacks on Sensor Networks using Dynamic Trust Management

[19] Sharmila, S., & Umamaheswari, G. "Detection of Sinkhole Attack in Wireless Sensor Networks Using Message Digest Algorithms" 2011 International Conference on Process Automation, Control and Computing, IEEE.

[20] Md. Ibrahim Abdullah, Mohammad Muntasir Rahman and Mukul Chandra Roy "Detecting Sinkhole Attacks in WSireless Sensor Network using Hop Count" I.J. Computer Network and Information Security, 2015 MECS.

[21] Imandi Raju and Pritee Parwekar "Detection of Sinkhole Attack in Wireless Sensor Network".

[22] Krontiris, I. Dimitrou, T. Freiling, F.C. (2007). Towards intrusion detection in wireless sensor networks. Proceedings of the 13th European Wireless Conference, Paris, France, April 2007.