AN EFFICIENT ANONYMOUS AUTHENTICATION SCHEME TO IMPROVE SECURITY AND PRIVACY IN SDN BASED WIRELESS SENSOR NETWORKS

Indira K
Research Scholar, School of Computing,
Sathyabama Institute of Science and Technology, Chennai, Tamilnadu, India
indira.it@sathyabama.ac.in

Sakthi U
Associate Professor, St.Joseph's Institute of Technology
Chennai, Tamilnadu, India
sakthi.ulaganathan@gmail.com

Abstract - Nowadays, software defined networking (SDN) model can sustain potentially support and flexible routing in various communication patterns that occur in wireless sensor networks (WSN). But implementing this model to resource-constrained networks is not direct, particularly if security services are an essential. For WSN existing SDN-based approaches developed addressing resource-constrained requirements and over time. Still in their implementation and design they do not integrate security services. In this paper we propose, an efficient anonymous authentication scheme to enhance security and privacy in SDN based WSN (SDWSN). The proposed method has perfect forward secrecy, achieve user anonymity and at the same time resistance to attack. For the resource constrained sensor nodes, it is very suitable. Also, a secure and efficient protocol for SDWSN is designed to detect and prevent security threads like flooding, replay and poison attacks which is due to lack of source authentication. Experimental results show the efficiency and effectiveness of proposed method in terms of delay, energy consumption, throughput, Packet Delivery Ratio (PDR) and packet loss. The proposed method is implemented utilizing NS-2 simulation and compared with existing protocol named lightweight anonymous authentication protocol (LAAP) and demonstrates our proposed method works better.

Keywords: Software defined network; wireless sensor network; SDWSN; attacks; delay; lightweight anonymous authentication protocol;

1. Introduction

Wireless Sensor Networks (WSN) is made out of resource constrained devices, from the environment with the motivation behind data gathering [1-3]. About the world, these devices can process, communicate and sense, perception and increment data. In WSN there are numerous applications, in which information source authentication, integrity and information confidentiality are the vital security services. The conventional networks security mechanisms can cause unwanted impacts like increment in communication delay/energy consumption from the processing overhead. For the execution of security mechanisms in WSN one of the fundamental difficulties is to illuminate the conflict between maximizing security and minimizing resource consumption [1, 5]. In correspondence protocols deployment moreover attributes like heterogeneity and mobility present new difficulties. For WSN routing protocols advanced over time. For example, in occasion and intrigue based networks coordinated diffusion was structured [6], exclusive traffic pattern of CTP (Collection Tree Protocol) is satisfactory [7], and to address diverse routing patterns like communication of node-to-sink, sink-to-node and node-to-node Ten RPL (RFC6550) was presented [8]. In any case, in node to-sink traffic it is intended to be proficient.

The security services arrangement and routing flexibility issues can potentially be tended to by the supposed SDN [9, 10], a worldview to control the network conduct that utilizes logically centralized software. For the SDN southbound protocol the broadly realized implementation is Open Flow [11, 12], with devices which has been utilized on wired networks and engaged with more resources generally. Something else, SDN for a WSN scenario forces distinctive requirements and challenges. The restricted resources are featured among the difficulties, for example, memory, processing, communication and energy. To the applications qualities like information size and frequency, operating systems, programming approach and nodes behavior due to duty cycles the requirements are connected.

The literature presents the SDN approaches when connected to WSN-like situations. Tragically there are drawbacks for these methodologies. The OPENFLOW have presented overhead, TCP use as basic communication protocol and issues concerning frame sizes. For download and utilize the SDN-Wise execution isn't totally accessible. Moreover, by plan none of these methodologies think about security. Along these lines a malicious node could attack the network causing routing holes and control messages are not authenticated. To the best of our knowledge, none of them address methodology for secure node admission, distribution of end-to-end key which are the requirements of modern security.

In the past several years, for WSNs many anonymous authentication schemes using lightweight cryptographic primitive have been proposed. However, most of them suffer from de-synchronization attack or cannot consider perfect forward secrecy. In this paper we propose, an efficient anonymous authentication scheme to enhance security and privacy in SDN based WSN (SDWSN). The proposed method has perfect forward secrecy, achieve user anonymity and at the same time resistance to attack. For the resource constrained sensor nodes, it is very suitable. Also, a secure and efficient protocol for SDWSN is designed to detect and prevent security threads like flooding, replay and poison attacks which is due to lack of source authentication. Rest of the paper is organized as follows: Section 2 presents the brief review of recent research works. The detailed procedure of the proposed scheme is presented in section 3, section 4 depicted results and discussion and finally, section 5 concludes the paper.

2. Related Work: A Brief Review

Various research works have already existed in the literature, which depend on security and privacy in software defined networking based wireless sensor networks with different perspectives. A portion of the works is reviewed on here.

The few security shortcomings of the previously mentioned plan were analyzed by Sooyeon and Taekyoung [13]. At that point, for the combination of 5G networks and WSNs the authors plan appropriate network design. Likewise, in their work a key assertion conspire in 5G-integrated WSNs and two-factor authentication for IoT was presented dependent on the engineering of network, that oppose different attacks including unlink ability, earlier distinguishing proof, and protect security prerequisites. Finally the authors assess the introduced technique execution and security and contrasted their scheme and other related plans. By utilizing opportunistic routing for point-to-multipoint in theory Xiaoyang Lai et al. [14] investigates the performance of broadcast data dissemination. Counting the priority scheduling algorithm and the distributed cooperation conspire the creators introduced another protocol named Receiver Negotiation Opportunity Broadcast (RNOB). Exploratory results showed, than traditional protocols the performance of RNOB is better and enhance data transmission efficiency and dependability in IoT systems of WSNs.

The difficulties and issues experienced in the usage and structure of PL-SKG conspires on off-the-shelf WSN was talked about by Kemedi et al. [15]. At that point a novel key generation conspire was presented by taking favorable circumstances of both the power and classic error correcting codes effortlessness, and furthermore the accessible frequency channels diversity on 802.15.4 compliant nodes, from Received Signal Strength (RSS) readings to create keys. For tackling the issue of Traffic Load Minimization (TLM) in SDWSNs, Guozhi et al. [16] presented a Flow Splitting Optimization (FSO) algorithm by thinking about the optimal splitting flow transmission and the optimal relay sensor node selection. At this end, authors initially set up the model of various packet types and depict the issue of TLM. In their work, by the packet likeness between various sensor nodes and the load of sensor nodes they define the issue of TLM as optimization issue. To deal with symmetric key distribution and node admission, a secure SDN structure named WS3N was exhibited by Renan et al. [17].To give services, cryptographic algorithms and protocols were joined with a SDN protocol.

Gope and Hwang [18] have presented a realistic anonymous user authentication in WSN. Basic conspicuous security issue, authors make an underlying move to shed light on the rationale. At first, so as to do that, the current answers for anonymous user authentication in WSN were show by authors were illogical. Also, a realistic authentication protocol (for WSN) was presented and guarantees different imperative security properties like un-traceability, user anonymity, perfect forward secrecy, forward/backward secrecy, and so forth. A trial show of software-defined-radio-based wireless tomography utilizing computer-hosted radio devices called USRP (Universal Software Radio Peripheral) was displayed by Jason Bonior et al. [19]. Inside a RF anechoic chamber automatic information acquisition was performed. For target imaging the born iterative strategy was used and for phase retrieval, semi definite relaxation was utilized. Turki A. Alghamdi [20] have introduced a secure routing and optimized energy protocol utilizing DHM (Dij-Huff Method). In the introduced method from source to destination, node with maximum energy will partake in the information transfer process.

2.1. *Background of the Research Work*

In network computing, the SDN brings about configuration in network computing, simplicity in network management, and innovation. Because of the rigidity of the network traditional networks often lack the flexibility to bring into effect instant changes. Thus moving the control logic from the node to a central controller, from the data plane, the SDN decouples the control plane. The WSN is a great platform for low-rate wireless personal area networks with short communication ranges and little resources. However, it faces several challenges like heterogeneous-node networks and network management, as the scale of WSN expands. Thus, to alleviate most of the challenges the SDN based WSNs are used. The combination of these two models gives rise to a new paradigm called SDWSN. In the following segment, we present the framework architecture and how it meets these necessities

3. Proposed Methodology

In this section, an efficient anonymous authentication scheme to enhance security and privacy in SDWSN is proposed. The software design for sensor nodes and the network controller is presented. The proposed method has perfect forward secrecy, achieve user anonymity and at the same time resistance to attack. For the resource constrained sensor nodes, it is very suitable. Also, a secure and efficient protocol for SDWSN is designed to detect and prevent security threads like flooding, replay and poison attacks which is due to lack of source authentication.

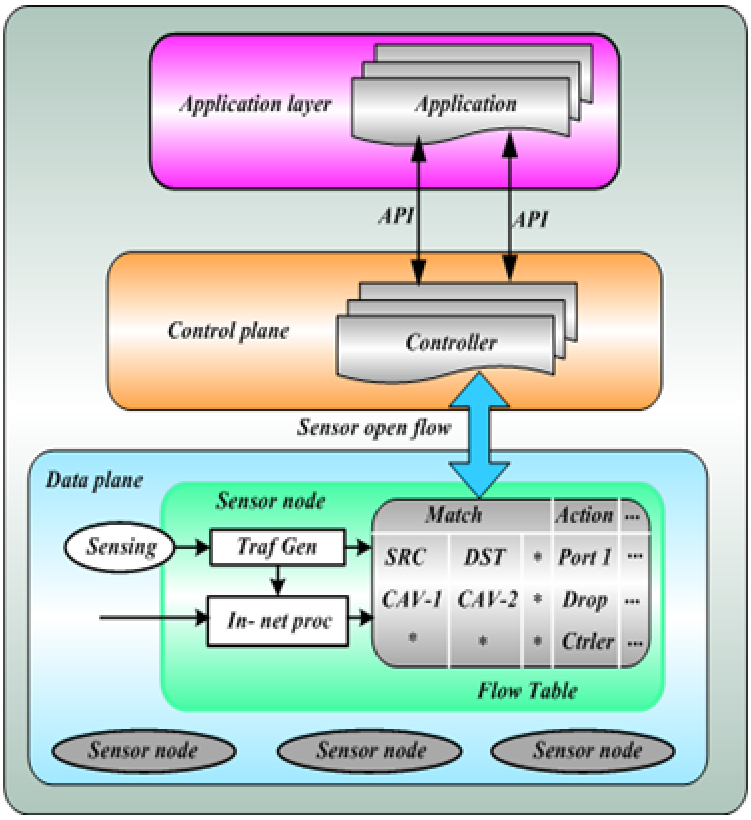

Fig. 1. Structure of Software Defined Wireless Sensor Networks.

The proposed secure privacy scheme consists of following stages. They are registration stage, authentication and login, and password update. In our research, the registration stage consists of two stages, such as user registration stage and sensor node registration. Information about these two stages is explained as given below.

3.1. *Registration Stage*

3.1.1. *User Registration Stage*

At first user is requested to register in GWN, when a user US_i need to access a sensor node sn_i. A smart card will be issued by the GWN, as an acknowledgement to the user US_i who requested for registration. The procedure of user registration phase is

Layer1:

A random number B_i is created by a new user US_i based on the selected id_i and password pw_i. Through a secure channel, US_i evaluates $c_i = H_0(id_i \| pw \| B_i)$ and US_i transmits to GWN is $\{id_i, c_i\}$

Layer2:

In the user information table, the GWN checks for the availability of id$_i$. GWN rejects the request of the user, if the id$_i$ present in the table. Or else, three random numbers are created by GWN USi, A, B, and sets $nc_i = A, \quad pid_i = pid_{i0} = B, \quad pid_{i1} = \perp,$

And evaluates $k_i = H_1(id_i \,\|\, X \,\|\, US_i), \quad f_i = k_i \oplus c_i$, $v = H_2(H_3(k_i \,\|\, c_i))$, and null is represented by $\perp$. Then the user identity information table is renovated by GWN, with the new entry

$$\{pid_{i0}, pid_{i1}, id_i, nc_i, US_i\},$$

and stores $\{pid_i, f_i, nc_i, v\}$ into smart card (SC). At last, through a private channel SC is send to the US$_i$ by the GWN.

Layer 3:

US$_i$ stores Bi into SC, once SC is received from the GWN.

3.1.2. *User Registration Stage*

In this phase sn$_j$ is required to register in GWN, when a new sensor node sn$_j$ is deployed. The following layers describe the procedure of sensor node registration phase.

Layer 1:

Through a secure channel, the new sensor node sn$_j$ choose identity sid$_j$ and transmits $\{sid_j\}$ to GWN.

Layer 2:

In the user information table, the GWN checks for the availability of sid$_i$. GWN rejects the request of the user, if the id$_i$ present in the table. Or else, a random number is created $k_{GWN-s,}$ and sets the starting sequence numbers $ns_j = ns_{j_0} = 0$.

Then the user identity information table is renovated by GWN, with the new entry $\{sid_j, ns_{j0}, k_{GWN-s}\}$ and sends $\{ns_j, k_{GWN-S}\}$ to sn$_j$ through a private channel.

Layer 3: The ns$_j$ from GWN after receiving k_{GWN-S} , as secret sn$_j$ stores them into its memory.

3.2. *Authentication Stage*

In this stage, if, he/she needs to achieve mutual authenticate with GWN and snj, then the user USi desires the WSNs service. The authentication procedure for the proposed method is illustrated as follows.

Layer 1:

In the smart card SC, if USi inputs id$_i$ and pw$_i$. The SC estimate

$$V = H(id_i| \; |c_i) \oplus n_i, m_i^{'} = H(c_i| \; |V), \; c_i = H(pw_i| \; |B_i)$$

and with the stored value mi it compares mi. The SC terminates the session if they are not equal. Otherwise as a legitimate user the SC believes USi. After that, a random number r1 is generated by SC and calculate

$$ct_1 = e_{E_K}(Did_i| \; |r_1| \; |t_1), E_K = H(Did_i| \; |V| \; |t_1), Did_i = H(id_i| \; |r_1).$$

Here, the timestamp is denoted as t1. At last through the public channel the SC sends the login request $\{Did_i, ct_1, t_1\}$ to the GWN.

Layer 2:

The GWN first check the t1 timestamp after the login messages are received and calculate

$$Did_i| \; |r_1| \; |t_1 = D_{E_K}(ct_1), E_K = H(Did_i| \; |H(X_i)| \; |t_1).$$

Further, with the received values the GWN check whether t1and Didi matches. The GWN terminates the session if they does not hold. Else, a random number r2 is generated by GWN and evaluate

$b_i = H(Did_i| \; |sk| \; |H(k_{GWN-S}| \; |sid_j)| \; |sid_j| \; |t_2), S_K = H(Did_i| \; |H(k_{GWN-S}| \; |sid_j)| \; |r_2| \; |t_2),$
$ct_2 = r_2 \oplus H(X_s| \; |sid_j).$

Here, the timestamp is denoted as t$_2$. At last the GWN transfer $\{Did_i, ct_2, t_2, b_i\}$to the sn$_j$ (sensor node).

Layer 3: From GWN upon receiving the messages, $\{Did_i, ct_2, t_{2i}, b_i\}$the timestamp t$_2$ is initially checked by the sn$_j$ and evaluate

$$r_2 = ct_2 \oplus H(k_{GWN-S}| \, |sid_j), S_K = H(Did_i| \, |H(k_{GWN-S}| \, |sid_j)| \, |r_2| \, |t_2),$$
$$b_i^{'} = H(Did_i| \, |sk| \, |H(k_{GWN-S}| \, |sid_j)| \, |sid_j| \, |t_2).$$

The sn$_j$ checks whether b $^{'}_{i}$ matches with the received b$_i$. The sn$_j$ terminate the session if it do not hold. Else,

$$c_i = H(H(k_{GWN-S}| \, |sid_j)| \, |sk| \, |Did_i| \, |sid_j| \, |t_3)$$

is computed by sn$_j$. Here, the timestamp is denoted as t$_3$. At last, the sn$_j$ send $\{c_i, t_3\}$to the GWN.

Layer 4:
In this step, the timestamp t$_3$ is initially checked by the GWN and calculate

$$c_i^{'} = H(H(k_{GWN-S}| \, |sid_j)| \, |sk| \, |Did_i| \, |sid_j| \, |t_3).$$

After that, with the received c$_i$ the GWN check whether $c_i^{'}$ matches. The GWN terminates the session if it do not hold. Else, GWN estimates $ct_3 = e_{E_K}(Did_i| \, |sid_j)| \, |sk| \, |r_1| \, |t_4)$. Here, the timestamp is denoted as t_4. At last, GWN send $\{ct_3, t_4\}$to US_i.

Layer 5:
In the last step, the US$_i$ checks the t$_4$ timestamp and evaluated with

$$Did_i| \, |S_{id_j}| \, |sk| \, |r_1| \, |t_4 = D_{E_K}(ct_3).$$

Then, with the previous values US$_i$ checks whether t$_4$, r$_1$, and Did$_i$ matches. The US$_i$ finishes the authentication if it holds the value. Else, US$_i$ miss for GWN authentication.

3.3. *Password Update Stage*

If USi need to renovate the password, user needs to run the steps given below.

Layer 1:
In this step, id$_i$ and pw$_i$ are the two inputs send to SC by the US$_i$. SC evaluates

$$c_i = H_0(id_i \parallel pw \parallel b_i)$$

And then the stored value v is compared with $v^{'}$. If values are not equal, SC fails to authenticate US$_i$, and rejects the password renovate request. Or else, new password $pw*i$ is given as input by US$_i$.

Layer 2:
The SC evaluates

$$c_i^* = H_0(id_i \parallel pw_i^* \parallel b_i), \; f_i^* = k_i \oplus c_i \oplus c_i^*, v^* = H_2(H_3(k_i| \, |c_i^*))$$

Layer 3: At last, to replace f_i and v, f_i^* and $v*$ are stored in SC.

4. Security Protocol for SDWSN Design

This section analyses the ability of the proposed method to resist various known attacks. A secure link discovery in SDWSN confirms minimum resource wastage of CPU, minimum bandwidth and exact topology discovery. Therefore, no optimal CPU and bandwidth usage are attained with the current extensions of security. In literature the authors defined the effects and threats of the security in SDWSN. However, the security threats are feasible to execute static packet creation, packet integrity check, and source authentication because of controller's inability.

For SDWSN security, to source switch and link discovery protocol packet is send by the packet sender sensor node. The eligible port identifier is an USP (unique selling proposition) of method, for each iteration it recognizes eligibility. The list is updated after each iteration in which all ports are considered initially. In the protocol when the switch rouses, in the eligible port (E-Ports) list its every port is added. Hence, for each eligible port including the latecomers of the previous cycle, in the next cycle the SLDP packets are generated

[21]. In our research the flooding attacks is detected for SDWSN security. The algorithm 1 shows the steps for detecting flooding attacks.

```
Algorithm 1: Flooding attacks detection
Require: SLDP Packet, Maximum Ports, E-Ports
Flood Detect process:
    In every received SLDP Packet
    EXTRACT(SLDP Packet) $\longrightarrow$ DP-ID, port-ID
    If   count for(DP-ID, port-ID)>Maximum Ports
         then
         Update:  e-Ports(E-Ports, port-ID, Remove)
    End if
End process
```

In algorithm 1, the suspicion is generated if the number of SLDP packets and port-ID (any switch port) are received more than the maximum number of ports on available switch (Maximum Ports). Then, periodically the SLDP generate packet one for each port, also if any port receiving more than Maximum Ports is eligible for removal.

5. Experimental Results and Discussions

In this section, we perform several experiments to evaluate the effectiveness of proposed methodology in SDWSN. The proposed method is simulated using NS-2 (Network Simulator) tool. The evaluation metrics like delay, packet delivery ratio (PDR), packet loss, energy consumption, and throughput are used to analyzed the proposed method performance and compared with LAAP [22] existing techniques. The simulation parameters of the proposed method are shown in Table 1.

TABLE 1. Simulation parameters of proposed method

Parameters	Values
Simulation Area	(1000×1000) m
MAC	IEEE 802.11n Physical
No. of Users	20, 40, 60, 80, and 100
User Mobility	10 m/sec
Range of Transmission	250m
Transfer Power of User	17 dBm
BW (Bandwidth)	20 MHz
Transfer power of base station	20 dBm
Size of Packet	1024 bytes
Traffic Source	CBR (Constant Bit Rate)
No. of frames per packet	Five

The performance of delay with respect to varying nodes is shown in fig 2. From the figure, it is clearly depicted that the delay of proposed algorithm is very low of 93.1% for 20 nodes, 96.8% for 40 nodes, 96.6% for 60 nodes, 97.04% for 80 nodes and 96.3% for 100 nodes when compared with LAAP algorithm.

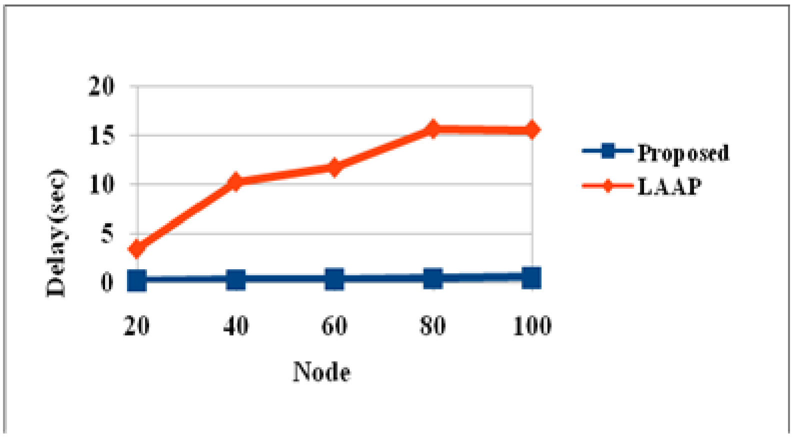

Fig. 2. Performance analysis of delay with various nodes

Fig 3 shows the performance analysis of packet delivery ratio with various nodes. It is clearly observed from the figure, the PDR of the proposed algorithm is better of 30% for 20 nodes, 63.6% for 40 nodes, 42.5% for 60 nodes, 81.2% for 80 nodes and 79.6% for 100 nodes when compared with LAAP algorithm.

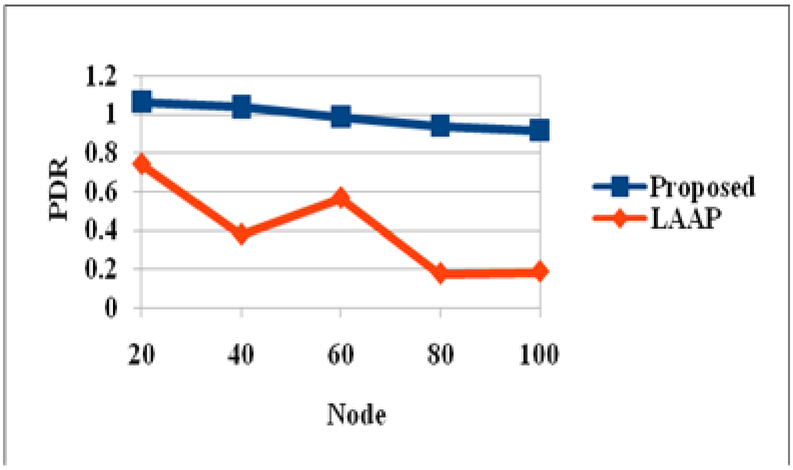

Fig. 3 Performance analysis of PDR with various nodes

The performance analysis of energy consumption with various numbers of nodes is shown in fig 4. From the figure, the energy consumption of the proposed algorithm is very less of 41.6% for 20 nodes, 41% for 40 nodes, 39% for 60 nodes, 25.5% for 80 nodes and 22.5% for 100 nodes when compared with LAAP existing algorithm.

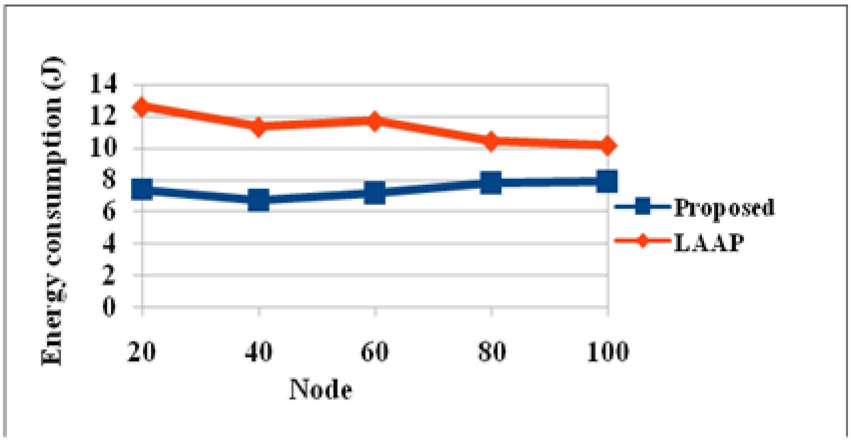

Fig. 4 Performance analysis of Energy consumption with various nodes

Similarly, the performance analysis of throughput with various nodes is shown in fig 5. The throughput of the proposed method is higher of 48% for 20 nodes, 47.8% for 40 nodes, 45.6% for 60 nodes, 36.7% for 80 nodes and 37.8% for 100 nodes when compared with LAAP existing algorithm.

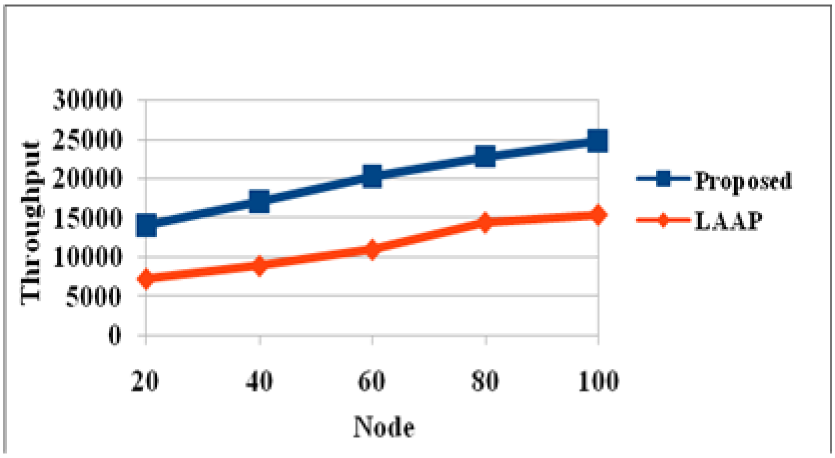

Fig. 5 Performance analysis of Throughput with various nodes

The performance analysis of packet loss with various nodes is shown in fig 6. From the figure, the packet loss of the proposed method is very less of 73.3% for 20 nodes, 96.4% for 40 nodes, 95.3% for 60 nodes, 94.3% for 80 nodes and 93.4% for 100 nodes when compared with LAAP existing algorithm. Thus, the packet loss of proposed method decreases with increasing number of nodes.

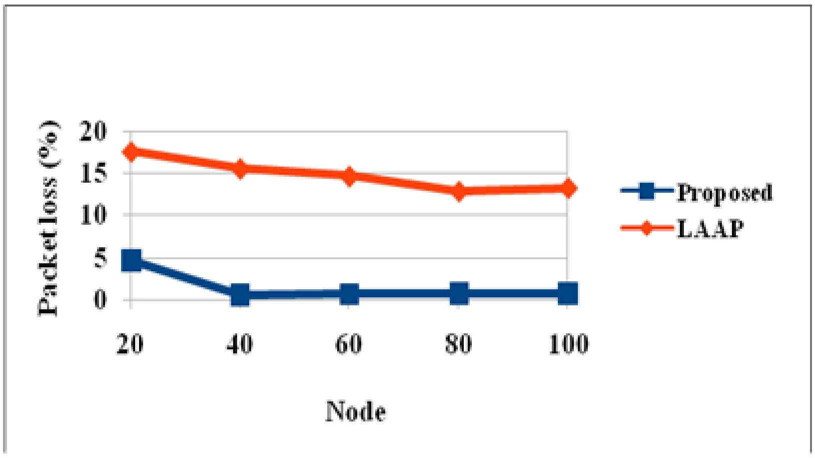

Fig. 6 Performance analysis of packet loss with various nodes

6. Conclusion

In modern WSN the flexibility and security are the essential elements. We dispute that SDN are efficient of assuming the desired flexibility. Nevertheless, in constrained devices the literature related to SDN application the security was not a concern. This paper algorithms and cryptographic protocols were integrated with an SDN protocol to satisfy such service was presented. Through an experimental setup we validated our proposed method. Simulation result shows that our proposed method outperforms better in terms of delay, packet delivery ratio, packet loss, energy consumption and throughput when compared with other state of art approaches. The delay of proposed method is low when compared with LAAP technique. The throughput of proposed method is better of 48%, 47.8%, 45.6%, 36.7% and 37.8% for varying nodes when compared with LAAP existing research works.

References

[1] O. Flauzac, C. Gonzalez, A. Hachani and F. Nolot, "SDN Based Architecture for IoT and Improvement of the Security", 2015 IEEE 29th International Conference on Advanced Information Networking and Applications Workshops, 2015.

[2] V. Tadinada, "Software Defined Networking: Redefining the Future of Internet in IoT and Cloud Era", 2014 International Conference on Future Internet of Things and Cloud, 2014.

[3] A. Mahmud and R. Rahmani, "Exploitation of OpenFlow in wireless sensor networks", Proceedings of 2011 International Conference on Computer Science and Network Technology, 2011.

[4] F. Hu and N. Sharma, "Security considerations in ad hoc sensor networks", Ad Hoc Networks, vol. 3, no. 1, pp. 69-89, 2005.

[5] G. Pereira, R. Alves, F. Silva, R. Azevedo, B. Albertini and C. Margi, "Performance Evaluation of Cryptographic Algorithms over IoT Platforms and Operating Systems", Security and Communication Networks, vol. 2017, pp. 1-16, 2017.

[6] C. Intanagonwiwat, R. Govindan and D. Estrin, "Directed diffusion", Proceedings of the 6th annual international conference on Mobile computing and networking - MobiCom '00, 2000.

[7] O. Gnawali, R. Fonseca, K. Jamieson, M. Kazandjieva, D. Moss and P. Levis, "CTP", ACM Transactions on Sensor Networks, vol. 10, no. 1, pp. 1-49, 2013.

[8] P. Rajakumar, R. Puviyarasi and S. Singh, "Power Management and Advanced Metering Infrastructure Using Wireless Network in Remote Areas", 2018 International Conference on Power, Energy, Control and Transmission Systems (ICPECTS), 2018.

[9] L. Galluccio, S. Milardo, G. Morabito and S. Palazzo, "SDN-WISE: Design, prototyping and experimentation of a stateful SDN solution for WIreless SEnsor networks", 2015 IEEE Conference on Computer Communications (INFOCOM), 2015.

[10] B. Trevizan de Oliveira, L. Batista Gabriel and C. Borges Margi, "TinySDN: Enabling Multiple Controllers for Software-Defined Wireless Sensor Networks", IEEE Latin America Transactions, vol. 13, no. 11, pp. 3690-3696, 2015.

[11] N. McKeown et al., "OpenFlow", ACM SIGCOMM Computer Communication Review, vol. 38, no. 2, p. 69, 2008.

[12] T. Luo, H. Tan and T. Quek, "Sensor OpenFlow: Enabling Software-Defined Wireless Sensor Networks", IEEE Communications Letters, vol. 16, no. 11, pp. 1896-1899, 2012.

[13] S. Shin and T. Kwon, "Two-Factor Authenticated Key Agreement Supporting Unlinkability in 5G-Integrated Wireless Sensor Networks", IEEE Access, vol. 6, pp. 11229-11241, 2018.

[14] X. Lai and H. Wang, "RNOB: Receiver Negotiation Opportunity Broadcast Protocol for Trustworthy Data Dissemination in Wireless Sensor Networks", IEEE Access, vol. 6, pp. 53235-53242, 2018.

[15] K. Moara-Nkwe, Q. Shi, G. Lee and M. Eiza, "A Novel Physical Layer Secure Key Generation and Refreshment Scheme for Wireless Sensor Networks", IEEE Access, vol. 6, pp. 11374-11387, 2018.

[16] G. Li, S. Guo, Y. Yang and Y. Yang, "Traffic Load Minimization in Software Defined Wireless Sensor Networks", IEEE Internet of Things Journal, vol. 5, no. 3, pp. 1370-1378, 2018.

[17] R. Alves, D. Oliveira, G. Pereira, B. Albertini and C. Margi, "WS3N: Wireless Secure SDN-Based Communication for Sensor Networks", Security and Communication Networks, vol. 2018, pp. 1-14, 2018.

[18] P. Gope and T. Hwang, "A Realistic Lightweight Anonymous Authentication Protocol for Securing Real-Time Application Data Access in Wireless Sensor Networks", IEEE Transactions on Industrial Electronics, vol. 63, no. 11, pp. 7124-7132, 2016.

[19] J. Bonior, Zhen Hu, T. Guo, R. Qiu, J. Browning and M. Wicks, "Software-Defined-Radio-Based Wireless Tomography: Experimental Demonstration and Verification", IEEE Geoscience and Remote Sensing Letters, vol. 12, no. 1, pp. 175-179, 2015.

[20] T. Alghamdi, "Secure and Energy Efficient Path Optimization Technique in Wireless Sensor Networks Using DH Method", IEEE Access, vol. 6, pp. 53576-53582, 2018.

[21] A. Nehra, M. Tripathi, M. Gaur, R. Battula and C. Lal, "SLDP: A secure and lightweight link discovery protocol for software defined networking", Computer Networks, vol. 150, pp. 102-116, 2019.

[22] L. Xiong, D. Peng, T. Peng, H. Liang and Z. Liu, "A Lightweight Anonymous Authentication Protocol with Perfect Forward Secrecy for Wireless Sensor Networks", Sensors, vol. 17, no. 11, p. 2681, 2017.

[23] Albert, R.; Jeong, H.; Barab´asi, A.-L. (1999): Diameter of the world-wide Web. Nature, 401, pp. 130–131.

[24] Berry M. W., Dumais S. T., O'Brien G. W. (1995): Using linear algebra for intelligent information retrieval, SIAM Review, 37, pp. 573-595.

[25] Bharat, K.; Broder, A. (1998): A technique for measuring the relative size and overlap of public Web search engines. Computer Networks, 30(1–7), pp. 107–117.

[26] Broder, A.; Kumar, R.; Maghoul, F.; Raghavan, P.; Rajagopalan, S.; Stata, R.; Tomkins, A.; Wiener, J. (2000): Graph structure in the Web. Computer Networks, 33(1–6), pp. 309–320.

[27] Chakrabarti, S. (2000): Data mining for hypertext: A tutorial survey. SIGKDD explorations, 1(2), pp. 1–11.