EAI Endorsed Transactions
on Internet of Things
Research Article EAI.EU

Secure ID-Based Routing for Data Communication in IoT

Madhusudan Singh,
Yonsei Institute of Convergence Technology, Yonsei University, Songdo, Incheon, South Korea

Abstract

Internet of Things is rising technology that could inspire the way wireless network access is provided. In IoT, secure data communication has lot of research scope. Especially message authentication, authorization cure path for IoT devices still remains as an open research problem. Some researcher proposed security mechanism without certification, MIC and token but still we didn't find standard security mechanism for data communication between sensor nodes. In this article author has proposed an Identity based security (IBS) mechanism for IoT devices during data communication in IoT networks. IBS mechanism uses identity-based cryptography (IBC) to avoid certificates, MIC and tokens to minimize the computational overhead. IBS Mechanism is resistant to most common security attacks such as modification, fabrication, replay attacks and it can also protect hop count. It does provide secure data communication between sensor nodes. The results, based on NS-3 simulation, reveal that proposed mechanism is effectively able to protect the black hole attacks. In results, we have shown the packet delivery ratio, quality of services (QoS), and throughput between IBS mechanism, AODV path and AODV with black hole.

Received on 13 June 2017; accepted on 18 October 2017; published on 15 January 2018

Keywords: Internet of Things (IoT), WSN, Security, Computing, path protocol, Adhoc Networks, WMN.

doi:10.4108/XX.X.X.XX

I. INTRODUCTION

The Internet of Things (IoT) word means, in this world every object is connected with Internet where connectivity and computing extends to sensors, items (smartphone, car, Cloths etc.) to allow to generate, communicate and consume data with minimal human intervention. Currently several leading Industries are linking object to object such as smartphones, cars, sensors and home appliances to the internet. Due to large amount of connectivity among objects, data amount generation is very high so data security of IoT is major research topic for companies and users. The attributes of IoT implementations, always introduces new and unique security challenges [1-2]. Wireless Sensor Network (WSN) is a new emerging and attractive communication technology for the next generation to provide better services. Wireless Sensor Networks (WSNs), consisting of wireless access networks interconnected by a wireless backbone, present an attractive alternative [3]. Compared to optical networks, WSNs have low investment overhead and can be rapidly deployed. The wireless sensor network structure is self-organizing, self-optimizing, and fault tolerant. WSNs have combine concepts from a diverse set of existing and emerging internet of things (IoT) including machine to machine, ad hoc networks, and sensor networks [2]. The application of research results from these areas could greatly contribute to the secure information sharing in IoT applications development, implementation of wireless Sensor networks based IoT architecture. [3] A common scenario of WSNs is the existence of an infrastructure that is further extended by ad hoc sub-networks. Within the infrastructure component, dedicated hardware may be assigned for path purposes; client nodes within the ad hoc network on the other hand are left to perform the path responsibilities. path and security requirements should be treated differently when addressing different components within a WSN. [4]

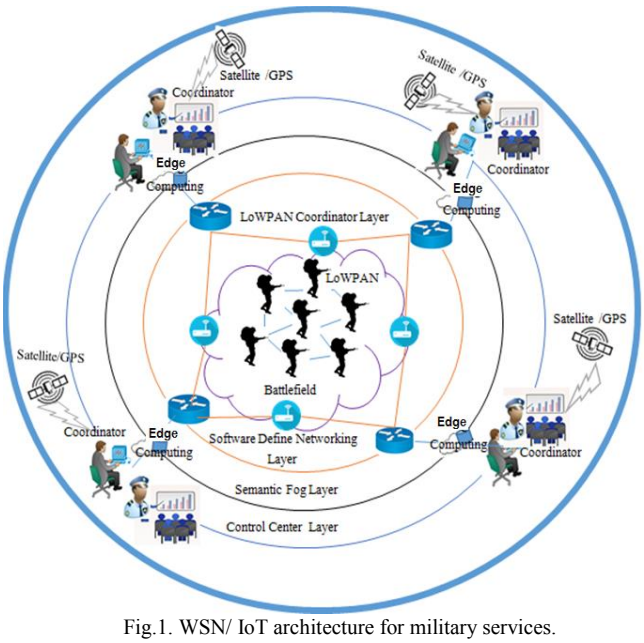

Fig.1. WSN/ IoT architecture for military services.

Security is an essential component of WSN to deal with various threats on path as well as on data packet transmission [5]. SIDBRM is a secure path protocol for WSNs. SIDBRM is a variant of AODV path protocol with added security features. It uses IBC to simplify the key setup among the clients without using digital certificates. SIDBRM is different from SAODV

which uses public key cryptography for protecting the path packets. [1].

In this paper we discuss some problem of SIDBRM. Section I we describe Introduction, section II discuss background study, section III analyze the security issues in SIDBRM, section IV specified problems with SIDBRM, section V provides possible solution, and last section VI we conclude our paper.

II. Related work and Challenges

SIDBRM has the following design goals: i) To avoid digital certificates and to simplify key setup using IBC; ii) To provide security against modification, fabrication, replay, and impersonation attacks on Domain-Sensor path; iii) To achieve the path at low computation and communication overhead, as well as with minimum latency [6]. There are three types of entities.

OPERATOR: The entity which operates a wireless Sensor network. A wireless network may contain single domain or multiple domains of different scales, either physically adjacent or non-adjacent. Operator is responsible to setup and maintain different agents or routers. Operator is also responsible for IBC domain parameter setup, and distribution of client ID, public key, and private key among the registered clients.

SENSOR ROUTER/AGENT (A): The entity that controls a single domain. An agent is under the administrative control of an operator. An operator which has multiple domains has multiple agents, one per domain. A Sensor router that can provide Internet connectivity to Sensor clients is called Sensor gateway router. A Sensor router/agent that cannot provide Internet connectivity directly but can offer Internet connectivity through nearest gateway router is called Sensor router.

SENSOR CLIENT (SC): The entity that wants to participate either in Domain-Sensor path or wants to have wireless Internet connectivity through agent. Each SC should belong to an administrative domain called its home domain.

DOMAIN-SENSOR COMMUNICATION: When any authorized client S wants to communicate with another client D within the same domain and if Path to D is not known, SIDBRM invokes path discovery mechanism similar to AODV [7]. SIDBRM uses similar mechanism as in with modifications to protect hop count.

PATH DISCOVERY: The path discovery process uses secure path request (SPREQ) and secure path reply (SPREP) packets. SPREQ packet format is similar to AODV's PREQ packet except for the following modifications: i) uses ID of MC instead of IP address; ii) uses no hop count field; iii) includes Neighbour Table NT, which contain the IDs of two recently traversed clients; and, iv) includes time stamp of source client. PREQ and TS are protected by the signature of source client with its private key i.e. K_s^{-1} [5~9]. If client S wants to send a packet to client D and if the path to client D is not available, S initiates SPREQ. The NT in SPREQ is initialized with the source client's ID and the time stamp TS is appended. The static parts of SPREQ are protected with light weight identity based signature because client S cannot calculate the shared key with the client D at this moment. S broadcasts SPREQ to its neighbours as in (1).

$$S \to *: K_s^{-1} R\,\mathrm{Re}\,q, TS), NT\{S\} \qquad (1)$$

Any 1st hop neighbour 'A' which is not the destination client, does the following in addition to the operations performed in the conventional AODV [7]: i) client A verifies the sign and authenticates S; ii) appends its ID to the NT; iii) marks its first hop neighbour in its table; and, then iv) broadcasts the message to its neighbours as in (2).

$$A \to *: K_s^{-1} SRREQ, TS), NT\{S, A\} \qquad (2)$$

Any neighbour B which is neither the first hop neighbour of S nor the destination client, records the second hop neighbour's ID in its path table [10].

Also, client B, removes from NT the reverse 2nd hop client's ID (i.e., S), and appends its ID as in (3), because NT holds IDs of two recently visited clients only.

$$B \to *: K_s^{-1} SRREQ, TS), NT\{A, B\} \qquad (3)$$

Finally, SPREQ reaches destination client 'D'. Client D makes similar entries in its Path table. Client D validates the signature and authenticates client S. Client D unicasts SPREP as in (4) back to the source

$$D \to B: SRREP, NT\{D\}, MIC_S, \mathrm{MIC_D}, \mathrm{H_{DB}}, \mathrm{H_{AD}} \qquad (4)$$

As in the case of SPREQ packets, SPREP packet format is similar to AODV's SPREP packet except for the following modifications: i) uses ID of MC instead of IP address; ii) uses hop count field; iii) includes Neighbour Table NT {}, which contain the IDs of two recently traversed clients; iv) includes message integrity check codes MIC_S, $\mathrm{MIC_D}$; and v) hash codes generated by two recently traversed clients to protect the hop count and other fields of SPREP. Client D sends SPREP to B as in (5) after the following operations: i) hop count initialized to zero; ii) NT is initialized with the destination client's ID; iii) calculates Token $Token = H_1(TS \| \mathrm{K_{SD}}), \mathrm{MIC_S} = H_1(SREQ \| \mathrm{Token})$ and $MIC_D = H_1(SRREP \| \mathrm{Toekn})$ with zero hop count; and, iv) appends keyed hash values H_{DB}, H_{DA} where B and A are the one hop and two hop neighbours respectively. Since D knows their identities from the SPREQ packet and it can calculate the shared key pair with each of them with the help of bi-linearity described in (1), the hash values are calculated as $H_{DB} = H_1(SRREP \| \mathrm{K_{DB}}$, and $H_{DA} = H_1(SRREP \| \mathrm{K_{DA}})$

These hash values are used to protect the hop count field from modification attack. Since, hop count value at two hop neighbour is exactly one less than the value at one hop neighbour, as the packet traverses from destination to source, every intermediate client checks whether the same difference is maintained by the two hash values calculated by successive clients. Client B verifies only H_{DB} because it has no two hop neighbour. Intermediate client B records the first hop neighbour, MIC_S and MIC_D in its Path [5].

Client B appends its hash values calculated with its reverse neighbours A and S as in (5)

Client A does' similar verification as done by client B. Finally, client. A unicasts the packet to client S as in (6).

$$A \rightarrow S : \text{SPREP, NT}\{\text{B, A}\}, \text{MIC}_{\text{S}}, MIC_D, H_{B,S}, H_{A,S} \quad (6)$$

Client S validate MIC_S, MIC_D and verifies $H_{B,S}$ and $H_{A,S}$. Now S can select the lowest hop count path from the received SPREP messages as the Path for its data transmission. Hop count modification is not possible because, every intermediate client checks the hop count information given by two most recently traversed clients.

After the validation of MIC_D, S authenticates D thereby completing the mutual authentication. Now all the intermediate clients have to authenticate source and destination clients. For this purpose, source attaches a token to the data packet. Upon receiving the data packet, every intermediate client performs the following operations: i) extracts the token from the data packet; ii) if token matches the one in its table then the packet will be routed according to the next hop entry in the table. If no token found in its table, then it proceeds as follows: i) calculates $MIC_S^1 = H_1(SPREQ_1 \parallel \text{Token})$ and compares with the recorded MIC_S; ii) If they are same it authenticates the source. Similarly it authenticates client D by checking MIC_D, if both the verifications are satisfied intermediate client records the token in its table [10].

PATH MAINTENANCE: Every client along the path monitors the connectivity between itself and next hop during the data packet transmission. If a client X observes link failure, it sends a path error message R_{err} to the source client after attaching MIC $_{err} = H_1 (R_{err} \parallel T_x \parallel K_{XS})$ Secure data packet transmission: After path setup, every data packet sent along the Path carries: i) Token; and, ii) H_1 (Data $\parallel K_{SD}$). Every intermediate client checks the validity of token, to verify the authenticity of packet's origin. The destination client validates the token and hash code of source client before accepting the data packet. This process adds minimal communication overhead to carry token, but gives no room for attacks on the Path and data [11].

III. Requirement and Challenges of Proposed Protocol

The proposed protocol is secure against most of the external attacks, because of the following defence mechanisms: A Sensor client is permitted to participate in the path protocol only after successful registration with its Operator. This process helps: i) To filter out external malicious clients from entering the network; and, ii) To bind a unique IP address with the ad hoc ID of the client. IP address is not only useful to uniquely identify the client in the global communication scenario but also helps to fix accountability to the participating clients [12]. Any registered client found guilty can be fixed and such clients can be eliminated from the network. This enhances trust levels among the members of the network. Path request packet has only static fields and that is protected by signature to detect tampering by intermediate clients and to ensure that the message is originated by authorized client. Path reply carries the hop count field which is the only mutable part. It is protected by two independent message integrity check codes generated by two successive recently visited clients. This process avoids the non-colluding malicious client to carryout hop count modification attack [13]. Token based path avoids most of the potential modification and fabrication attacks on the source path because intermediate clients authenticate the path based on the token, which is not revealed until the exchange of Path request and Path reply has finished, and it is very hard to forge MIC_S and MIC_D without knowing the shared secret [14]. End-to-end authentication in the Path request phase avoids impersonation of source and destination clients. End-to-end integrity in the path request phase avoids modification attacks by intermediate clients. Hop-by-hop authentication in the path reply phase avoids external malicious clients to participate in the routing protocol and thereby avoids the attacks caused by them. SIDBRM is resistant to most common security attacks such as modification, fabrication, replay attacks and it can also protect hop count. But still SIDBRM have challenges [15].

SIDBRM PROBLEMS: SIDBRM is very good protocol. It has provided very strong security during domain Sensor communication against common attacks like modification, fabrication, replay attacks but still it has some challenging issues. Such as:

PROACTIVE SECURITY MECHANISM: Proactive security mechanism in SIDBRM protocol, operator provide unique id to each agent and each sensor clients before network establishment. Operator has each sensor agent and client's identity. But author didn't talk anything about after network establishment. Proactive security mechanism is a challenging issue as it is not always possible for the operator to involve and to watch out each agent and its activities. ADDED/DELETED NODE: SIDBRM is only talking about limited nodes. SIDBRM authors did not talk about the situation when a new node is added or deleted from the network then what will happen, how the new node will communicate in the network, how will his neighbour get information and if any node is deleted from the network then how it is deleted from the neighbours table, and how other nodes will know that his neighbour node was deleted from the network. So we can say that this is also a big challenge in the SIDBRM.

BLACK HOLE ATTACKS: SIDBR protocol provided security against many common attacks such as modification, fabrication, replay attacks but it is secure against black hole attacks. In black hole attacks, a malicious node advertises itself as having a valid path to a destination node. The node consumes the intercepted packets. Cooperative black hole: More than one malicious node in network. Those node works together in the network. SIDBRM is not protecting the network for this type of attack. Black hole attacks are very big challenge for SIDBR protocol.

NO ACKNOWLEDGEMENTS: SIDBR protocol did not discuss about any information during communication. After path establishment SIDBRM believes that route path is purely secure. Source node didn't get any acknowledgement form intermediate node or destination node. After path establishment, source node starts communication and it

assumes that the data is communicating in the correct path. This is also one issue in the SIDBRM.

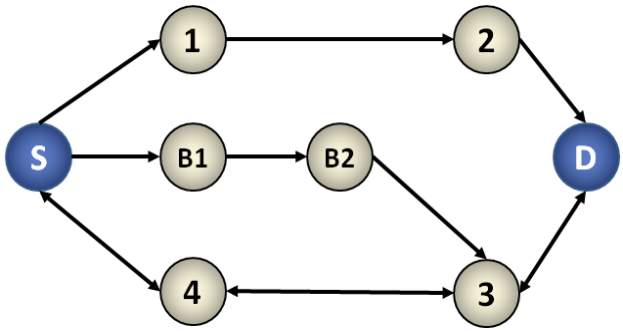

Fig.2. Cooperative Black hole

IV. PROPOSED SIDBR MECHANISM

PROACTIVE SECURITY MECHANISM: The Operator provides unique id to sensor agent and client according to SIDBR protocol before network establishment. Operator has each nodes id and it also take care of each agent and client. If there is any problem in system, then operator is responsible for solving the problem. We can slightly change the system by letting operator only provide the id to sensor agent and sensor agents providing unique id to sensor client. If any sensor client will have any problem, then the agent will be solving that problem without operator interference. With this techniques network will not been totally dependent on the operator and agents will have also some responsibility to take care of sensor client. After network establishment if any new sensor client or agent wants to involve in network then they can easily involve.

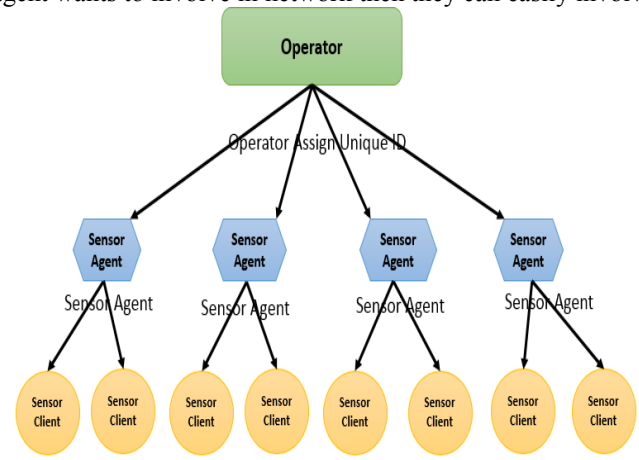

Fig. 3. Assigned unique ID by Operator and Sensor agents

ADD NEW NODE IN NETWORKS: SIDBRM did not discuss the case when any new node is added or deleted in the network. This challenge can remove from the SIDBRM with the help of sensor agent. If any new client wants to join network, then firstly the node need to register it by the sensor agent. After getting unique id, the node sends hello message to his neighbours. Each neighbour verifies his id with sensor agent. After that the neighbour's node adds him as neighbours. New node add process described in figure 4 (F) In figure 4 has described the complete work of Sensor Agent. In figure 4(A) has shown the new node addition, figure 4 (B) shows, registration of new node in Sensor Agent. In figure 4(C) to figure 4(F) has shown the communication and addition the neighbour's index. If any node wants to free from the network, then it will simply inform the sensor agent and leave the network. Sensor agent will then broadcast a refresh message to each node.

BLACK HOLE ATTACKS: SIDB routing protocol didn't provide security against black hole attack. A black hole has two properties. First, the node exploits the ad hoc routing protocol, such as AODV, to advertise itself as having a valid Path to a destination node, even though the Path is spurious, with the intention of intercepting packets. Second, the node consumes the intercepted packets.

The solution of black hole challenges to identify multiple black hole nodes acting in cooperation involving two bits of additional information from the nodes responding to the PREQ of source node S. Each node maintains an additional Data Routing Information (DRI) table. In the DRI table the first bit "From" stands for information on routing data packet from the node (in the Node field) while the second bit "Through" stands for information on routing data packet through the node (in the Node field) [2].

CROSS CHECKING: The source node (SN) broadcasts a PREQ message to discover a secure path to the destination node. The Intermediate Node (IN) generating the PREP has to provide its Next Hop Node (NHN) and its DRI entry for the NHN. Upon receiving PREP message from IN, the source node will check its own DRI table to see whether IN is a reliable node. If source node has used IN before to path data, then IN is a reliable node and source node starts routing data through IN. Otherwise, IN is unreliable and the source node sends forward request (FRq) message to NHN to check the identity of the IN, and asks NHN: 1) if IN has routed data packets through NHN, 2) who is the current NHN's next hop to destination, and 3) has the current NHN routed data through its own next hop. The NHN in turn responds with forward reply (FRp) message including 1) DRI entry for IN, 2) the next hop node of current NHN, and 3) the DRI entry for the current NHN's next hop. Based on the FRp message from NHN, source node checks whether NHN is a reliable node or not. If source node has routed data through NHN before, NHN is reliable; otherwise, unreliable. If NHN is reliable, source node will check whether IN is a black hole or not. If IN is a black-hole, the source node identifies all the nodes along the reverse path from IN to the node that generated the PREP as black hole nodes. Source node ignores any other PREP from the black holes and broadcasts the list of cooperative black holes [3]. Cross checking has shown in fig 10.

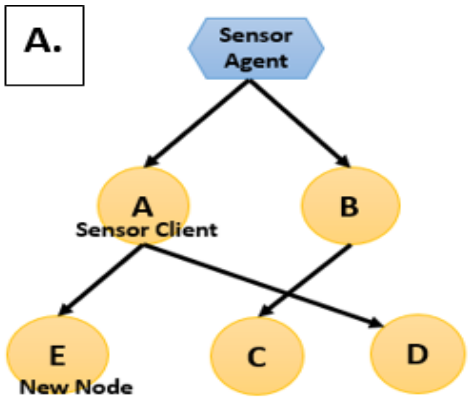

Fig.4(A). New node Request for joining network

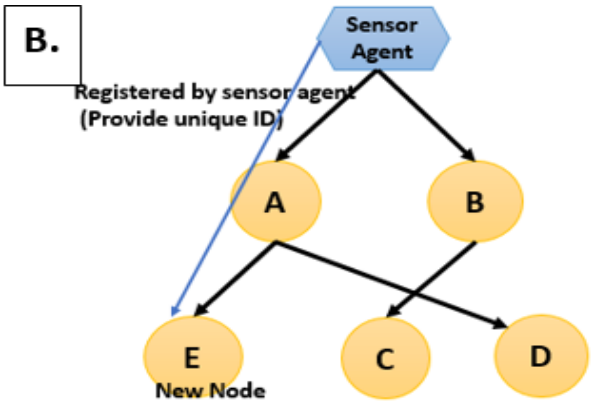

Fig. 4(B). Registered by Sensor agent

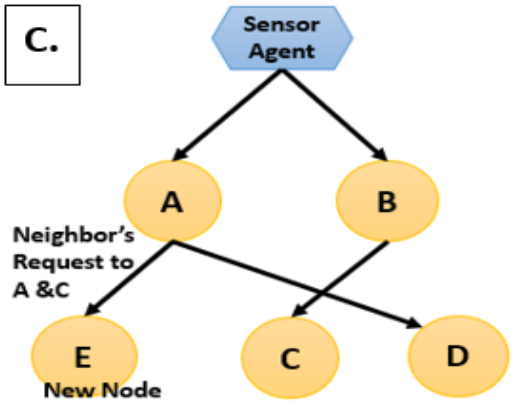

Fig. 4(C). Send Request to neighbors

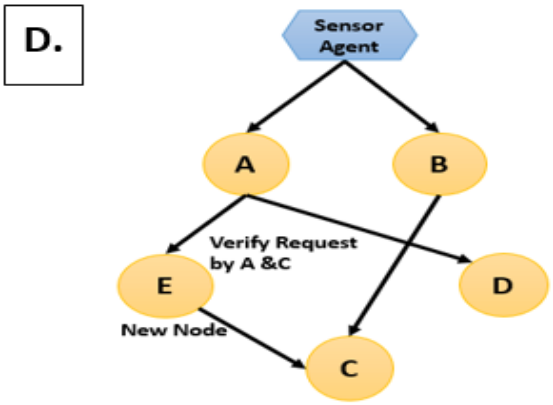

Fig. 4(D). Send verification request to sensor agent by Neighbours node

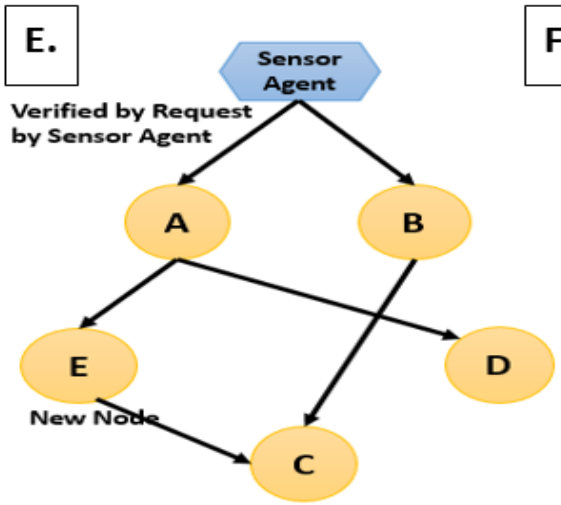

Fig. 4(E). Verified by sensor agent

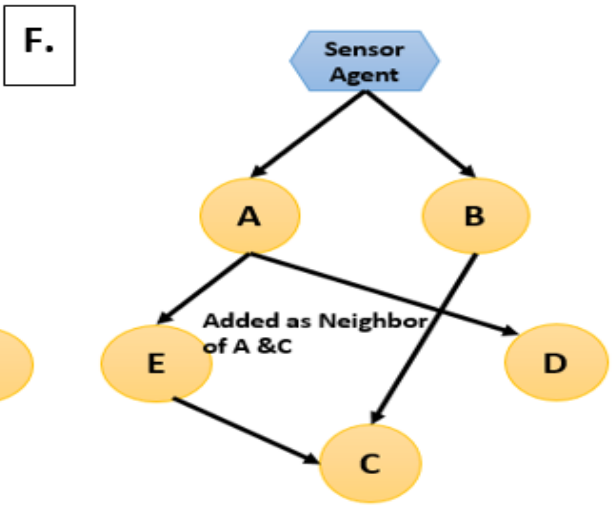

Fig. 4(F). Add as a neighbour

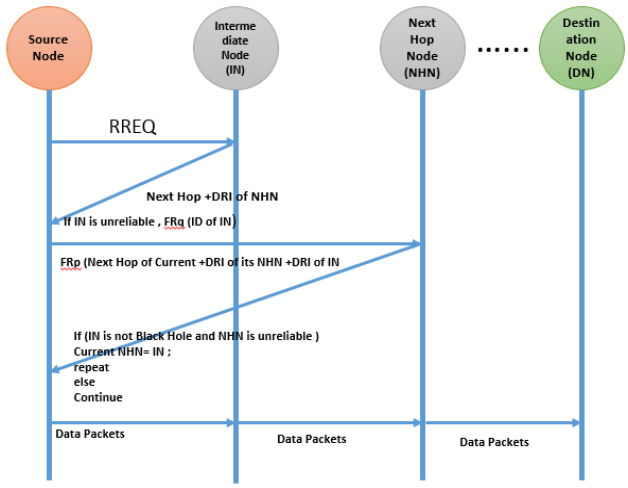

Fig. 10 Cross checking for Black hole nodes

NO ACKNOWLEDGEMENTS: This problem source node didn't know node sent packet on correct path or not. For this each next hope send acknowledgements signal to his previous node after getting packet. After that previous node checks his Path table and confirmed his packet traversed right node. In table 1 has shown the differences between Existing and proposed security mechanism

Table1. The differences between Existing and proposed security based routing mechanism

Features	Proposed Secure Identity Based Routing mechanism	Existing Secure outing Mechanism [Certificates, Key (public Private), MIC, Token]
Computation Overhead	Low	High
Time	Low	High
Power Consumption	Low	High
Reliability	High	High
Authentication	High	High
Memory space	Low	High
Data Execution Time	Low	High

V. PERFORMANCE ANALYSIS

In this analysis, we have shown the desultory weakness with and without and also propose PROTECTED DOMAIN method black hole attacks. It is an important analysis because it clearly proves that how much difference occurs during the node communications. So our method can provide smart secure communication in wireless communications for this type of attacks. Hence it becomes highly secure for the critical wireless networks applications to function on the IoT. We have simulated our proposed method on NS-3 simulator.

In these simulations, we have analysed packet loss and delay in packet transmission, QoS, and Throughput, which is not tolerable in critical networks application, and QoS throughput results with normal, with black hole and PROTECTED DOMAIN AODV routing method. The results in packet loss and delay in packet transmission are not tolerable in critical wireless networks Application. In figure 11, we have shown the ratio of packet delivery within 150 connected node based networks. We have found the packet delivery ratio between normal AODV, Black hole AODV, and our proposed security method for AODV (PROTECTED DOMAIN AODV or Protected local region). We have found a considerable amount of packet drop in percentage packet delivery during black hole attacks and there is potential drop in the network performance as soon as attack is introduced. But time based applications are not suitable for this condition. In that case, our propose methods provides secure data packet delivery without any loss of packet drop in network. Our proposed method provides local protection, not allowing any out sider of the network to attack network and also prevents the delayed packet delivery, ultimately depolarize the drop in the packet delivery.

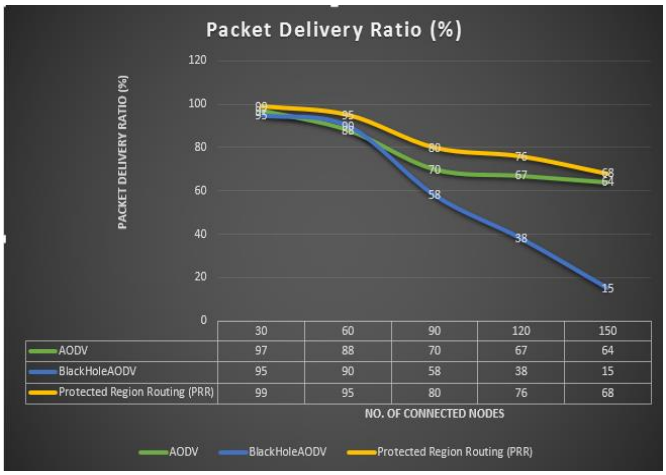

Fig.12. Packet Delivery Ratio

The simulation of Quality of Service guarantee of the network is shown in Figure 13. The Protected Region Routing provides at least a minimum of QoS guarantee to keep the network working securely.

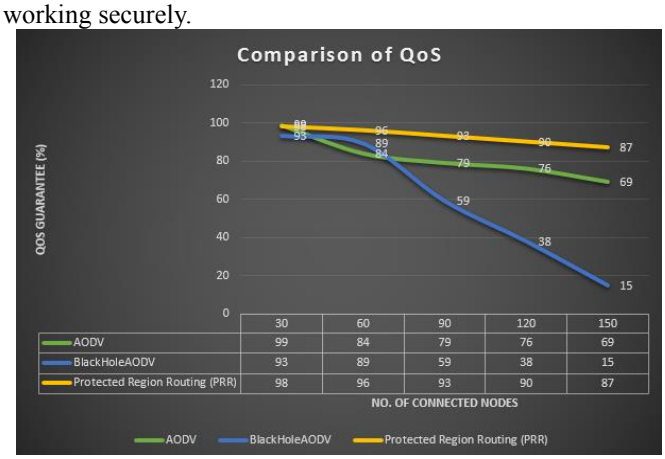

Fig.12. Comparison of QoS

The throughput analysis is shown in Figure 13, with respect to time. The Throughput of our propose security protocol increases without any downgrading at any point in the network. Thus, it provides security inside the network's environment and time check of the environment behaviour, ensuring the complete network security.

Fig.14. Throughput

VI. Conclusion

Secure data communication between sensor networks is a very crucial issue in manner of packet delivery, throughput and quality of services for wireless sensor application compare to existing routing protocols. We have demonstrated an identity based security mechanism enabled AODV routing protocol. Our proposed mechanism gives better packet delivery, throughput and quality of services results compared to without security enabled mechanism. IBS mechanism uses identity-based cryptography (IBC) to avoid certificates, MIC and tokens, to minimize the computational overhead. IBS Mechanism is resistant to most common security attacks such as modification, fabrication, replay attacks and it can also protect hop count. It provides secure data communication between sensor nodes. Our results are based on NS-3 simulation. Our proposed mechanism effectively protects the black hole attacks.

Acknowledgment

This work was supported by Institute for Information & communications Technology Promotion(IITP) grant funded by the Korea government (MSIP) No.2017-0-00560), Development of a Blockchain based Secure Decentralized Trust network for intelligent vehicles)

References

[1] Hyun Seok Yoon, Dong Hwi Lee, Gangtaek Lee, Kuinam J. Kim, "A Study on the Information Superiority of Network Centric Warfare for Future Battlefield", International Conference on Information Science and Security, Seoul, 10-12 Jan. 2008, pp 224-231.

[2] Singh, D., Tripathi, G., and Jara, A. J., "A survey of Internet-of-Things: Future vision, architecture, challenges and services," in Proc. of the IEEE World Forum on Internet of Things (WF-IoT), pp. 287-292, IEEE, 2014.

[3] Vaquero, L.M., Rodero-Merino, L.: Finding your way in the Fog: Towards a comprehensive definition of fog computing. ACM SIGCOMM CCR 44 (2014).

[4] Zhang, Q., Cheng, L., Boutaba, R., "Cloud computing: state-of-the-art and research challenges", Journal of internet services and applications (1) (2010).

[5] Ramanarayana Kandikattu and Lillykutty Jacob, "A Secure Intra-domain Routing Protocol for Wireless Sensor Networks", ICISS 2007, LNCS 4812, PP. 37–50, 2007.

[6] Ramaswamy, Sanjay, Fu, Huirong, Sreekantaradhya, Manohar, Dixon,John and Nygard, Kendall E, " Prevention of Cooperative Black Hole Attack in Wireless Ad hoc network", in Proceedings of the International Conference on Wireless Networks, Las Vegas, June, 2003.

[7] Khin Sandar Win ,"Analysis of Detecting Wormhole Attack in Wireless Networks", World Academy of Science, Engineering and Technology (WASET journal) Vol.48, 2008

[8] Rusinek, D.; Ksiezopolski, B. On the Effect of Security and Communication Factors in the Reliability of Wireless Sensor Networks. J. Sens. Actuator Netw. 2014, Vol.3, 81-94, 2008.

[9] Sonia Waharte & Raouf Boutaba & Youssef Iraqi & Brent Ishibashi, "Routing protocols in wireless Sensor networks: challenges and design considerations", Springer Science + Business Media, LLC, July 2006.

[10] Georg Lukas, Christian Fackroth, "WMNSec – Security for Wireless Sensor Networks", IWCMC'09, Leipzig, Germany, June 2009.

[11] Buratti, C.; Conti, A.; Dardari, D.; Verdone, R. An Overview on Wireless Sensor Networks Technology and Evolution. Sensors2009, Vol. 9, PP. 6869-6896, 2009.

[12] Del-Valle-Soto, C.; Mex-Perera, C.; Monroy, R.; Nolazco-Flores, J.A. On the Routing Protocol Influence on the Resilience of Wireless Sensor Networks to Jamming Attacks. Sensors, Vol.15, PP. 7619-7649, 2015.

[13] M. Singh, D. Singh, A. Jara, "Secure cloud networks for connected & automated vehicles", IEE 2015 International Conference on Connected Vehicles and Expo (ICCVE), pp.330-335, 2015

[14] Chen, J.-L.; Ma, Y.-W.; Lai, C.-P.; Hu, C.-C.; Huang, Y.-M. Multi-Hop Routing Mechanism for Reliable Sensor Computing Sensors 2009, Vol. 9, ISSN: 10117-10135, 2009

[15] Kartsakli, E.; Lalos, A.S.; Antonopoulos, A.; Tennina, S.; Renzo, M.D.; Alonso, L.; Verikoukis, C. A Survey on M2M Systems for mHealth: A Wireless Communications Perspective. Sensors, Vol. 14, ISSN 18009-18052, 2014

[16] Ghayvat, H.; Mukhopadhyay, S.; Gui, X.; Suryadevara, N. WSN- and IOT-Based Smart Homes and Their Extension to Smart Buildings. Sensors 2015, Vol. 15, ISSN: 10350-10379, 2015.

[17] Mansour, I.; Chalhoub, G.; Lafourcade, P., "Key Management in Wireless Sensor Networks", Journal Sensor Actuator Network, Vol 4, PP. 251-273, 2015.