DAP-LECP: Dos Attack Prevention and Low Energy Consumption Protocol for Wireless Sensor Networks

Nasir Rashid
Department of CS and I.T, University of Malakand, KPK, Pakistan

Muhammad Salam
Department of CS and I.T, University of Malakand, KPK, Pakistan

M. Raees Khan
Department of CS and I.T, University of Malakand, KPK, Pakistan

Fakhre Alam
Department of CS and I.T
University of Malakand
KPK, Pakistan

ABSTRACT
The wide-spread deployment of wireless sensor networks (WSN) promises extensive applications in military and civilian fields. So far the major research focus has been to make WSN more useful and scalable in order to cope with future challenges of communication technologies, small emphasis is placed till now for the secure communication in WSN. A lot number of WSN protocols exist that have been designed to figure out the weaknesses and to provide feasible solutions concerning the security, Denial of service (DoS) attacks, data routing, data dissemination and power consumption. Our research work have analyzed a variety of key distribution and sharing protocols designed to detect and avoid DoS attacks in WSN. We propose a security protocol, modified form of identifier based protocol, for prevention of denial of service attack in WSN that provides a solution to battery exhaustion of sensor network by disseminating the identity of a malicious node.

Keywords
Battery exhaustion, denial of service, data routing, data dissemination, key distribution, malicious node.

1. INTRODUCTION
Wireless sensors are incorporated into structures, technology and hostile environments, tangled with an efficient transmission of the fully sensed information, and have the capability to provide splendid benefits to the modern society. Prospective benefits includes: conservation of natural resources, detection of floods, improving manufacturing productivity, habitat monitoring, battle fields monitoring and enriched homeland security [1].

Figure. 1 shows a common structure of WSN, which can be defined as a physical and logical network of connected sensor, denoted as nodes or smart dust, which have the capability to sense the critical environments and forward the gathered information from the observed fields of interest through wireless links using the RF channels [2, 3]. The data is communicated, probably through multiple links, to a sink (sometimes called as regulator or monitor). The monitor can be installed locally or is connected to other networks through a gateway [7]. Sensor nodes of the WSN are capable to move arbitrary with in the specified region of boundaries, however the nodes can also be stable. All the sensor nodes can have a critical knowledge of the surrounding environment. All these nodes of a particular sensor network can be of the same type.

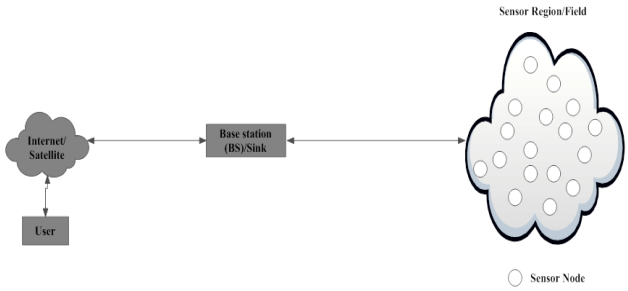

Figure 1. Typical Wireless Sensor Network Architecture

The major issues pertain to WSNs, that affect the design and performance are their low processing capability, low battery power and, deployment, localization, architecture, middleware, quality of service, physical security, heterogeneity of nodes and constrained resources are some areas of concern [5].

Deployment of sensor network is a labor intensive activity. As the infrastructure is not well defined, this behavior exposes the WSN networks to various security threats [6]. There are various defense mechanisms designed in order to provide possible solutions to most probable threats in WSNs. One of the feasible techniques is to provide security with obscurity in networks that consists of huge number of sensor nodes with high computation and processing capability [4]. In these highly dense sensor networks bandwidth and battery power is preserved due to the lack of proper security plan and low communication to exchange keys and security protocol data [10].

Public-key cryptography schemes are better solutions for keys generation, management and its distribution in old-fashioned WSN, however due to small memory and processing power of these motes , the possibility for using this scheme is no more feasible [11].

Rest of the paper is organized as follows. Section 2 provides details of the existing key distribution protocols regarding DoS and exhaustion of battery attacks. Section 3 outlines some of the problems in the discussed key distribution protocol. Section 4 proposes a security protocol for major problems identified in literature. Section 5 summarizes this paper with conclusions in and section 6 provides further study and research in related concerned field.

2. RELATED WORK
There are number of protocols available for WSN, but our primary focus has been on those that are concerned with the key distribution, scalability of WSN, security, broadcasting and prevention of DoS attacks.

2.1 Some Key Distribution and Broadcasting Protocols in WSN

SPIN-BC has been designed for broadcast wireless sensor networks, exclusively using cheap and one-to-many communication architecture. Broadcasting mechanism of SPIN-BC consumes very small amount of energy by disseminating the data. SPIN-BC motes coordinate their conserving efforts in more effective way. Each node eavesdrop all the communication patterns that do occur within the transmission range of a broadcasting node [18].

Sensor protocols for information through negotiation (SPINS) is a security protocol suite that have been designed for negotiating shared session key in wireless sensor networks. There are two major components of SPINS; SNEP and μTESLA. SPINS uses the trusted third party i.e. the Key Distribution Center (KDC) approach to create a session between motes or nodes [12]. KDC responsibility is to authenticate and generate the session keys and send these shared keys to communicating nodes. In this protocol, each sensor node communicates a secret key with a base station [13].

SNAKE is a protocol that can negotiate the session key in an ad-hoc fashion between the nodes in the wireless sensor networks [8]. SNAKE protocol does not need to depend on KDC as it is used in the SPINS. In this protocol the nodes prove its authenticity through a mutual verification process and in giving response to the challenge message. This is more scalable protocol than SPINS, because in this protocol there is no involvement of the KDC [9].

SEKEN exchanges secure keys between the neighbor motes by utilizing minimum amount of sensor node resources [14]. SEKEN is considered as a feasible protocol for the hierarchical based or tree-based network architecture with trusted base station. The overall communication takes place through the trusted base station deployed in this type of WSN [13].

BROSK is a new standard broadcasting Negotiation Protocol that is used for secure communication in different pattern WSN. According to the function of the protocol, each node communicates a session key with its surrounding nodes by sending a request message through broadcasting. BROSK follows the fully ad-hoc mechanism in order to communicate the session key process [15]. BROSK works well on the assumptions that a particular WSN that follows the mentioned protocol have limited resources, having static or very low mobility and all the nodes share a common master key.

IBKDP is an identity based key distribution protocol designed for WSNs. This protocol extracts the secret ID and node ID from the request message and compares the authentication process by comparing the extracted data with pre-stored database [16]. This protocol has been integrated with already existing WSN protocols like SPIN, BROSK and SNAKE in order to increase the functionality for detection of DoS attacks and has been designed for the purpose of battery exhaustion attacks.

2.2 Problems in WSN's Key Distribution Protocol

WSNs are more prone to severe security attacks and service degradation. Due to such attacks sensor node may lose energy due to over computation, processing of the wrong information, authentication, and transmission of the irrelevant data, which requires extra computational power and memory consumption [17].

The problem with SPINS is that it suffers from Denial of Service (DoS) attack. When a new mote from outside the predefined WSN network initiates a request to the target node, the target node forwards the same request to KDC that will have to perform the authentication [18]. A malicious node can send the same messages after short intervals continuously in less spam of time. The victim node will repeat the authentication process for each request message. Due to which the receiver node may lose energy gradually.

In BROSK when a sensor node broadcast their key sharing requests, there is no response for request. Due to the reason, such requests messages only update the session keys on receiver end and generation of new request is stopped. However this session key negotiating process could threaten the security of the whole WSN due to the insider attack because every request message received must have to be forwarded.

IBKDP has explored the weaknesses and problems with different WSN key session protocols in terms of DoS attacks and minimization of energy consumption level of a particular node. IBKDP is not scalable as the Secret ID has been taken to include only last 6 natural numbers whose sum must be equal to 39, so this mechanism can only generate 6!or 720 Secret IDs which limited the scalability of the sensor network. Authentication mechanism followed by IBKDP involves too much computation and requires more energy consumption in case if we have a large data base. There is no mechanism for the broadcast of malicious node's identity, so as to expose its presence, which can increase the life span of sensor's energy.

The SNAKE shared-session key protocol faces the Dos attack. In SNAKE, a malicious node initiates a request and sends it to the target node. The authenticity of the node can be proved if there is a proper reply for the challenge message. If a malicious node repeatedly sends the request within a limited time frame continuously, the victim node must also have to repeat the same process for the authentication. A lot of energy is wasted for processing the requests and there is no authentication of the new node.

3. PROPOSED PROTOCOL

A large number of key distribution algorithms exist for WSNs but the most desirable solution for resource starved sensor network is a scheme in which the keys are pre-distributed. Our proposed security protocol has taken care of denial of service attacks as well as for preserving the energy of whole cluster/network.

3.1 Protocol Architecture

This proposed security protocol has been integrated with existing key distribution and broadcasting protocols. Fig. 2 gives a pictorial presentation of proposed security protocol. Our protocol works on the validity of a node from which a request is generated for key negotiation. If this step fails then it discards further requests from the same node and its identity must have to be broadcasted with assumption of sensor node mobility.

3.2 Network ID

Network ID is automatically generated by a trusted base station that is installed in each node of WSN and is known by to the entire sensor network.

3.3 Node ID

Node ID is unique for every sensor node and is pre-deployed by the base station in the entire wireless sensor network.

3.4 Secret ID

The proposed protocol defines a 9-digit Secret ID (SID) for each sensor node. SID is composed of any grouping of natural numbers from 1 to 9 with no redundancy. SID is used to identify node of a sensor network at the time of request made for joining the WSN.

3.4.1 Secret ID Validation

Once the receiver node receives the request from the sender node, it separates network ID (Net-ID), Node ID (NID) and secret ID (SID) from that message. This protocol performs Pre-Storage Database Approach to validate the SID of a sensor node.

In case of Pre-Storage Database Approach, if SID does not match with available entries in the database, it stops receiving further requests from that particular node, as Net-ID and NID can be found matched. If SID matched with the database entry, further actions will be then carried. For the purpose of scalability, validation needs to be performed on algorithm basis. For this purpose the sum of digits (SID) is taken as 45, the SID is authenticated or otherwise request for key is discarded.

3.4.2 DOS Identification

If secret ID does not match with Pre-Storage Database identities, its intentions may be treated as malicious attack and system warning is generated against Denial of service attack .Our proposed protocol considers into account such types of attacks and hence the request is rejected. If SID of a requesting node is authenticated and log on, a timer is activated to count down the number of requests in a specified amount of time. If the number of requests exceeds a defined value, implies a DOS attack. SID of this malicious node will be stored in a separate database, named as MNodeDB, which is created in case of DOS identification. The victim node may then disseminate the SID of the same malicious node to all the neighbor nodes with the help of SPIN-BC protocol, designed for broadcasting with less energy consumption and without any redundancy. Keeping in view the mobility of malicious node in the area of interest, every sensor node in a network must have the information of the same malicious node in order to identify it easily and deny DOS attack. If the number of requests from the requesting nodes is less than some defined value then further processing will take place and session will be created for proper communication.

4. ALGORITHM

Denial of Service Attack in SPINS and SNAKE Protocols is described in below mentioned algorithm. (SecID, DBID, BEG, LB, END, UB, PT, NETID, NDID).Here SecID (Secret Identities) stored in database in the form of array with start LB and end UB. The variables DBID, NETID, NDID, and PT denote, the Database Identity, Network ID, Node ID, Beginning and End of database and protocol type respectively.

1. START = LBound, End = UBound
2. START: Send Request
3. Request received:
   Get NETID, NDID and SecID
4. Validate NETID and NDID
5. If NETID = = Network ID stored at Receiver Node
   Then go to step 6
   Else go to step 10
6. Repeat step 6 while Start < =END
   If (NDID = = DBNDIDS [START])
   "NDID Found" Go to step 7
   Else START = START+1
   Go to step 10
7. Repeat step 7 while START<=END
   If (SecID = = DBSecID [START])
   "SecID Found" go to step 8
   Else START=START+1
   [End of if structure]
   Go to step 10
   OR validate (SecID)
   If SUM (Digits(SecID)) = = 45) then go to step 8
8. Log the SecID and activate the timer
   If (No_of_Requests> =10&& Time> = 60 sec)
   Then display "DOS attack"
   Create MaliciousDB and store the SecID
   Broadcast SecID through SPIN-BC protocol
   Go to step 10
   Else go to step 9
9. If (PT=SPINS) then request KDC
   Else challenge request originator
   [End of if structure]
10. Exit

5. ANALYSIS

The proposed protocol works efficiently as compared to the discussed protocols in terms of security, scalability and battery exhaustion. This protocol has integrated SPIN-BC in order to disseminate the key information of malicious node in case of DOS attack to the whole cluster so that the overall performance and battery life should be maximized. The proposed protocol performs node authentication process with the help of simple algorithm that has been designed according to the limited memory and processing capability constraints of the sensor nodes.

6. CONCLUSION

Our work has explored different key distribution and broadcasting protocols designed for WSNs and have discussed various problems in these protocols. The main area of focus was the DoS attack and battery exhaustion attacks. We proposed a security protocol for the prevention of DoS attacks in particular and to preserve the energy of sensor nodes in general. This protocol is also a modified form of IBKDP which has been integrated with the existing key distribution and key broadcasting protocol of WSN.

7. FUTURE WORK

With the advancement in sensor network technology and rapid development of protocols, the possibilities of security threats also amplify. The development of a key management protocol is only first step in developing a suit of protocol for securing the WSNs of tomorrow. As new protocols develop in WSNs, the security threats become the challenging aspect for researchers. A lot research work is done regarding WSNs security and still more is required. Our designed protocol involves identification DoS attacks, minimization of authentication overhead, broadcasting the presence of malicious nodes to make protocol more efficient in resources utilization. The broader scope of WSNs in near future opens many new research areas to be explored. A more matured algorithm based protocol is needed to identify the DoS attacks in hybrid WSN architecture and enhance the life span of energy power of sensors during communication.

8. ACKNOWLEDGMENT
We are very thankful to our respected supervisor Dr. Muhammad Arshad for reviewing the paper and providing valuable suggestions.

9. REFERENCES
[1] Basagni, Herrin, C., Bruschi, D., and Rosti, E. (2001). Secure Pebblenets. 2nd International Symposium on Mobile Ad Hoc Networking & Computing. Washington, ACM.

[2] ErikOliver, Michael Conrad, Martina Zitterbart. "A tree based approach for secure key distriobution in wireless sensor networks." Real World Sensor Networks. June 2005.

[3] Cheng, Y., and D. P. Agrawal (2006). Distributed Pairwise Key Establishment in Wireless Sensor Networks, Nevada, USA, International Conference on Pervasive Systems Computing.

[4] D.EstrinL.Girod, G.Pottie, M.Srivastava, "Instrumenting the World with Wireless Sensor Networks", In Proceedings of IEEE ICASSP 2001, pp.2033-2036.

[5] Lewis, F. L.Wireless sensor networks. Wiley: D. J. Cook and S. K. Das, editors, Smart Environments: Technology, Protocols, and Applications, 2004.

[6] E.-O Blaß, M. C., and M. Zitterbart (2005). A tree-based approach for secure key distribution in wireless sensor networks. Real World Sensor Networks, Stockholm, Sweden.

[7] Seyit A. C. Amtepe and B. Ulent Yener, "Key Distribution Mechanisms for Wireless Sensor Networks: A Survey", Rensselaer Polytechnic Institute Technical Report TR-05-07, March 2005.

[8] W. Du, J. Deng, Y. S. Han, Shigang Chen, P.K. Varshney, "A Key Management Scheme for Wireless Sensor Networks Using Deployment Knowledge", IEEE INFOCOM 2004

[9] Bocheng Lai, Sungha Kim,Ingrid Verbauwhede. "Scalable Session Key Construction Protocols for Wireless Sensor Networks." IEEE,Large Scale Real Time and Embedded Systems. usa, 2002.

[10] William Stallings, "Cryptography and Network Security, Principles and Practice", Second Edition, Prentice Hall Publishing, ISBN-13: 9780130914293, 2001.

[11] R. L Rivest, A. Shamir, and L. M. Adleman, "A method for obtaining digital signatures and public-key cryptosystems", Communications of the ACM, vol. 21, no. 2, pp. 120–126, 197

[12] Adrian Perrig, Robert Szew czyk, J.D. Tygar, Victorwen and David E. Culler "SPINS: Security Protocols for Sensor Networks", Wireless Networks, Kluwer Academic Publishers Netherlands 2002. pp 521.534

[13] Bocheng Lai Sungha Kim, Ingrid Verbauwhede, "Scalable Session Key Construction Protocol for Wireless Sensor Networks", Report by Department of Electrical Engineering

University of California, Los Angeles, CA-90095.

[14] Schwiebert , Kamran Jamshaid and Loren. "Seken (secure and efficient key exchange for sensor networks)."IEEE International Conference, Computing, and Communications,. 2004. 415–422.

[15] Shan Jiang, Sean Smith, Kazuhiro Minami. "Securing Web Servers against Insider Attack." Computer Security Applications Conference. 2001. 131-141.

[16] Muhammad Adeel, Munir Hussain, Urooj Beenish, Shenila Mehwish, Laurissa Tokarchuk, Amer Shahzad. "Identifier Based Key Distribution Protocol for Wireless Sensor Networks." SoftCom, Software, telecommunications nd computer networks, 16th Conference. 2008.

[17] Chien -Chun Ni, Tien-Ruey Hsiang, J. D. Tygar. "A Power-Preserving Broadcast Protocol for WSNs With DoS Resistance." 17th International IEEE Conference on Computer Communications and Networks. 2008. 1-6.

[18] W. R. Heinzelman, and H. Balakrishnan, "Negotiation-Based Protocols for Disseminating Information in Wireless Sensor Networks," Wireless Networks, vol. 8, 2002, pp. 169–85.

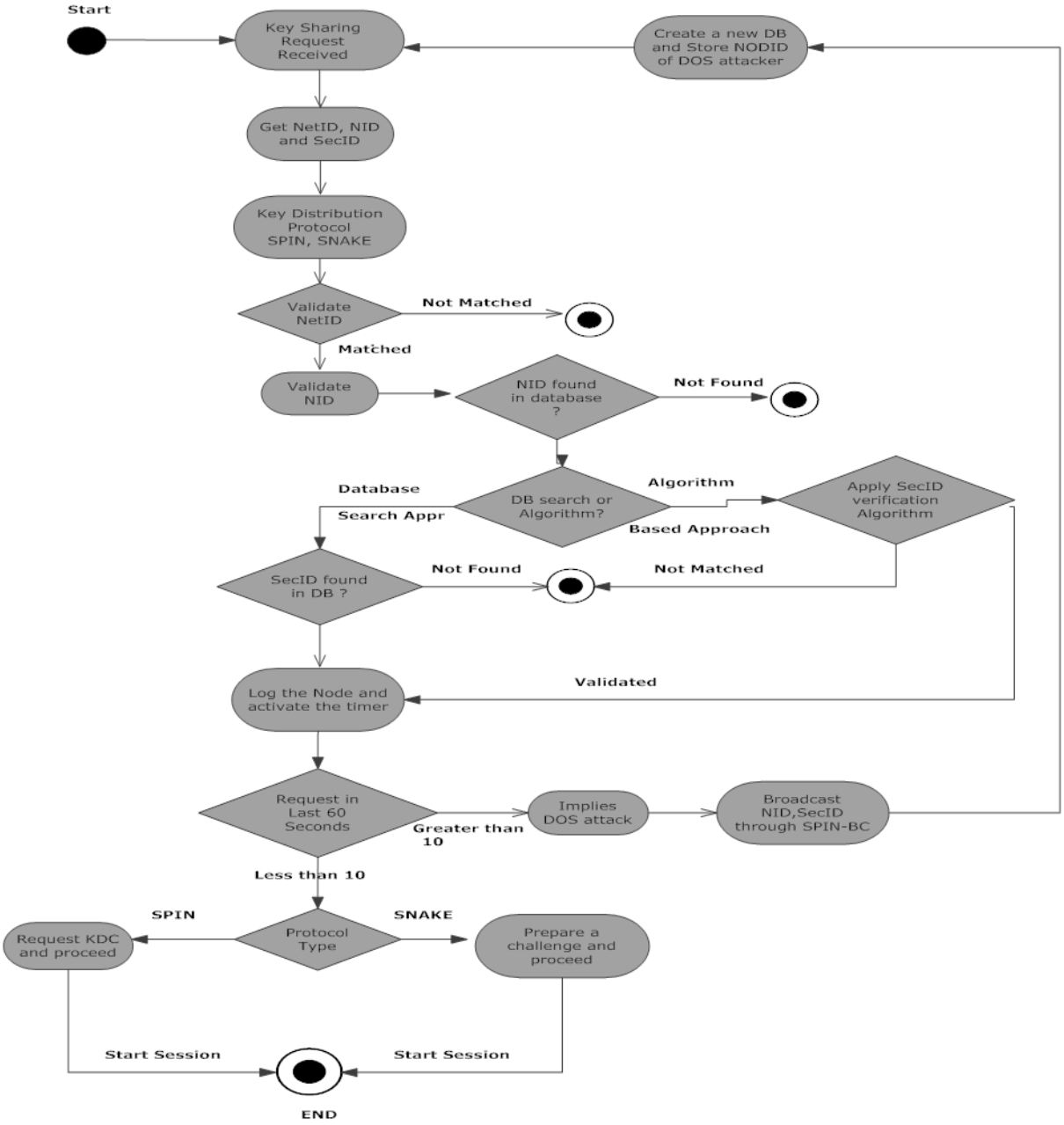

Figure 2. DAP-LECP Architecture