ANALYSIS OF QUERY BASED ATTACK IN THE DELAY/FAULT TOLERANT MOBILE SENSOR NETWORK

Rahul Johari[1]

[1]University School of Information Technology, GGSIP University, Dwarka , Delhi
rahuljohari@hotmail.com

ABSTRACT

The Delay/Fault Tolerant Mobile Sensor Network (DFT-MSN) and Mobile Peer to Peer network (MP2PN) have evolved at a tremendous rate in the last couple of years. As the networks are evolving so is the rate at which the queries are exchanged in between these network and the number of database accessess that need to be performed. The queries are getting complex due to the mobile nature of the nodes in these network and their eagerness to get the response accurately in short span of time because of their limited energy resources. In this paper the effort is made to depict the routing strategies prevalent in DFT-MSN using the OMNET++ , proposing a set of SQL/TIQL queries that are exchanged between the pair of nodes taken from the CRAWDAD dataset , portrays their execution on Oracle 9i Enterprise Edition Release 9.2.0.1.0 Production and expose how these queries are vulnerable to the different type of the SQL attack which can either be launched manually or through the various proprietary and open source SQL Injection tools.

KEYWORDS

DoS, ORACLE, OMNET++

1. INTRODUCTION

The Delay/Fault Tolerant Mobile Sensor Network (DFT-MSN) are established on adhoc basis without any pre-defined configuration. The DFT-MSN comprises of a wearable sensor nodes (source node) and the high end sink node(HES) [1].The source node takes the responsibility of the gathering data from its environment and relaying it to the high end sink node through direct transmission if the sink node is one hop away or through the multi-hop transmission if the high end sink node is distant away. This situation is similar to the Mobile Peer to Peer network (MP2PN) where the resource management and the network communication is multi hop [3].The High end Sink node are then further inter-connected to each other [7] or they can be connected to backbone access point where the received information is then filtered, processed and the analysed for decision making process [8] [9]. The analysed data are then stored in the in the local copy of the database at the high end sink node and the final results are stored in the global copy of the database stored at server which is connected via the backbone network access point or access point with sink node. The Source nodes can either be wore by human or they can be attached or plugged in via Crossbow imotes [10] or injected by means of a chip in animals (without injuring them) depending on whether the data to be gathered is from human populace or from animal habitation. Sun Spots [11] from SunMicroSystem is another recently in- troduced hardware device that is immensely popular in gathering information about neighbourhood environment.

DOI : 10.5121/ijasuc.2011.2410

Various Analytic models with several data delivery schemes (including direct transmission, Zebranet [12], South African Village [13] model Replication based Data delivery schemes) and nodal mobility patterns(such as uniform and power law distributions) have been proposed and implemented [13]. One of the pertinent question often posed in DFT-MSN type of network is that whether the Source node and Sink node is mobile or stationary, one of the pertinent answer is can be that it purely depends on the application in which they are deployed.

2. RELATED WORK

[5] is concerned with query processing in sensor networks. Researchers world- wide have noted the advantages of a query processor-like interface to wireless sensor networks and the need for sensitivity to limited power and computational resources.[4] suggests that the in-network query processing paradigm in sensor networks involves the concept that a query is routed among sensors and collects the answers from the sensors on its trajectory. It works for static and connected sensor networks. However, when the network consists of multiple number of mo-
bile sensors and is sparse, a different approach is needed. The author presents a idea that a query processing method uses cooperative caching. To cope with communication bandwidth and storage constraints, the method prioritizes the data-items in terms of their value, as reflected by supply and demand. The method of prioritization has been further taken on in [3]where in the
author presents an architecture for Tactical Information Middleware for bandwidth constrained information management. The author further proposes an idea of rank-based data dissemination, and the use of a SQL(Structured Query Language)/TIQL(Tactical information management query language) which would be responsible for the exchange of the data or information between the nodes. The author proposes a new application called CarTel [2] that they deployed on a set of six cars running on a small scale in Boston and Seattle for over a year. It has been used to analyze commute times, analyze metropolitan Wi-Fi deployments and for automotive diagnostics. CarTel applications run on the portal using a delay tolerant continuous query processor ICEDB to specify how the mobile nodes should summarize, filter and dynamically prioritize data. The portal and the mobile nodes use a delay tolerant network stack, CafNet to communicate.It is prepared in Microsoft Word as a .doc document. Although other means of preparation are acceptable, final, camera-ready versions must conform to this layout. Microsoft Word terminology is used where appropriate in this document. Although formatting instructions may often appear daunting, the simplest approach is to use this template and insert headings and text into it as appropriate.

3. ROUTING

For routing the packets IN DFT-MSN and MP2PN we use various techniques such as Direct transmission and the Epidemic Routing. Their functionality along with example is depicted as follows :-

3.1 **Case I** - Direct Transmission (Direct Routing), which can also be considered a degenerate case of the forwarding family, where it always selects the direct path between the source and the destination. Here we have a common sink for the adjacent four sources nodes and each source nodes is in direct contact with this sink. Whenever a source has some packets to transmit, it directly forwards the packets to the sink. Due to its simplicity, it does not consume many resources, and it uses exactly one message transmission. Here, we have a more numbers of sinks and each sink is attached to adjacent four sources as shown in figure below. For routing the packets IN DFT-MSN and MP2PN we use various techniques such as Direct transmission and the Epidemic Routing

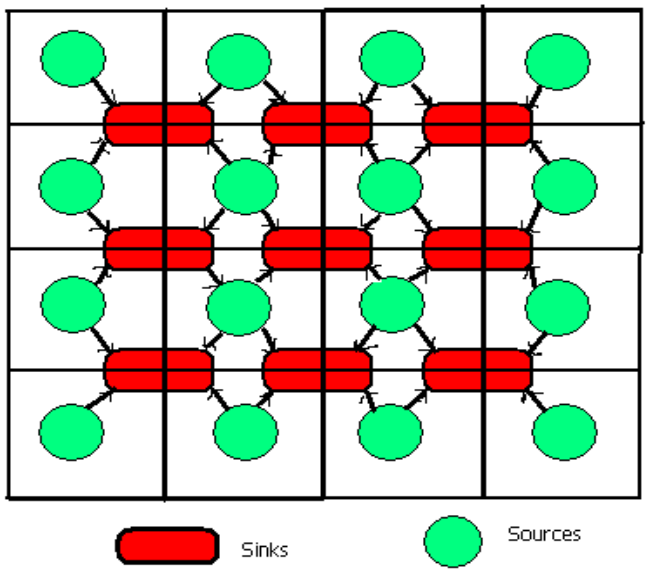

Figure – 1 : Schematic representation of One hop Routing

3.1.1 Application of Case Study 1 :-

A person goes for shopping in the mall, the source DTN node fitted in his car immediately comes in contact with the DTN node when he visits the parking bay for parking his car, the source node contacts the destination node of the control room of the parking plaza, if the parking slot is available then the detailed information viz. parking bay no, on which floor it is available i.e basement ,first floor and the approximate parking charges per hour for parking the car etc is all transmitted to the source node. This example illustrates how the information is communicated from source node to the destination node through one hop transmission.

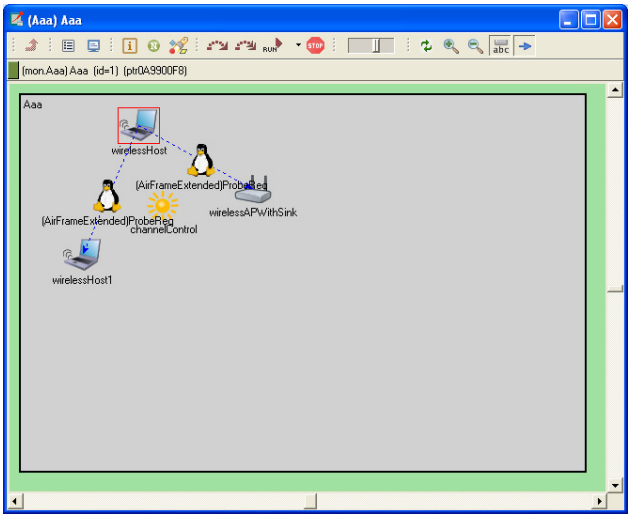

Figure – 2 : One hop Routing Simulation in OMNET++

3.2 **Case II -** Flooding strategy(Multi Hop routing) , which rely primarily on replicating messages to enough nodes so the destination receives it. Routing algorithm used in this type of strategy is called Epidemic. Epidemic algorithms guarantee that provided a sufficient number of random exchanges of data, all nodes will eventually receive all messages. Thus, the destination node is guaranteed to have received the data. Epidemic Routing works as follows. When a message is sent, it is placed in the local buffer and tagged with a unique ID. When two nodes connect, they send each other the list of all the messages IDs they have in their buffers, called the summary vector. Using the summary vector, the nodes exchange the messages they do not have. When this operation completes, the nodes have the same messages in their buffers. Epidemic Routing represents the extreme end of the flooding family because it tries to send each message over all paths in the network. This provides a large amount of redundancy since all nodes receive every message, making this strategy extremely robust to node and network failures. Additionally, since it tries every path, it delivers each message in the minimum amount of time if there are sufficient resources.

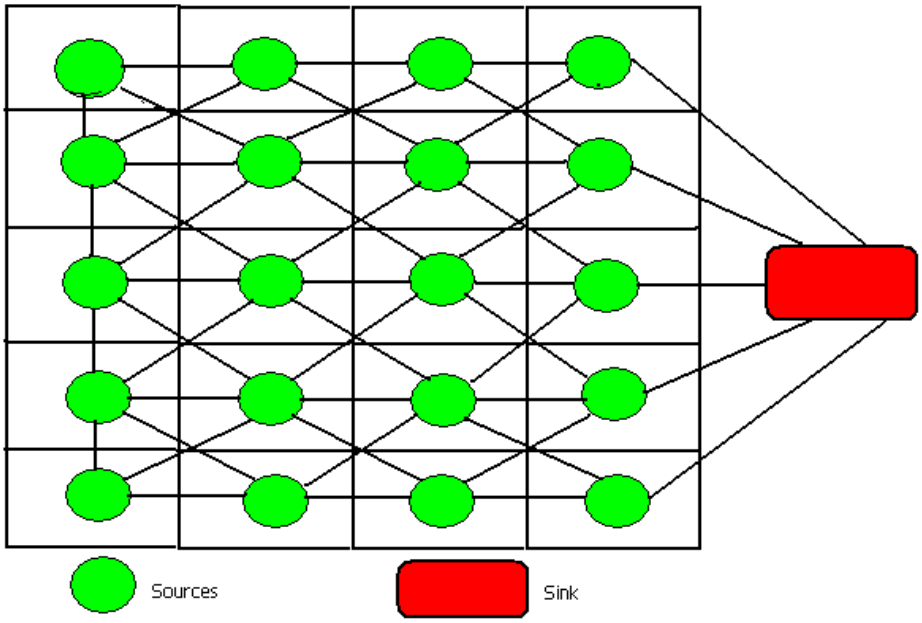

Figure – 3 : Schematic representation of Multi-hop Routing

3.2.1 Application of Case Study II :-

A Person is driving a car which is fitted with source DTN[19] node ,goes for shopping in the supermarket to buy a Trouser ,while shopping for trouser, he visualizes it that he intends to buy a shirt also so he generates the query which is broadcasted to all the neighbouring nodes so that the query propagates through multi-hop transmission and searches for all the available shops that sells the shirt of the brand X, the query reaches to the node that is closer to the shop that sells the Shirt of the brand 'X'. The destination DTN node sends the response as Yes to the Source DTN node .On receiving 'Yes' the Source DTN node further generates the query that the customer is looking for the Shirt with a specification of 40 no in size, Striped in type and blue in color ,the query corresponding to such a request is then transmitted via the reverse path back to the destination node and the response is then relayed back to the source node.

Epidemic Routing is relatively simple because it requires no knowledge about the network. For that reason, it has been proposed to use it as a fallback when no better method is available [9]. The disadvantage is that a huge amount of resources are consumed due to the large number of copies. This requires large amount of buffer space, bandwidth, and power. Many papers have studied ways to make Epidemic Routing consume fewer resources. Epidemic flooding can be understood as shown in figure below [10].

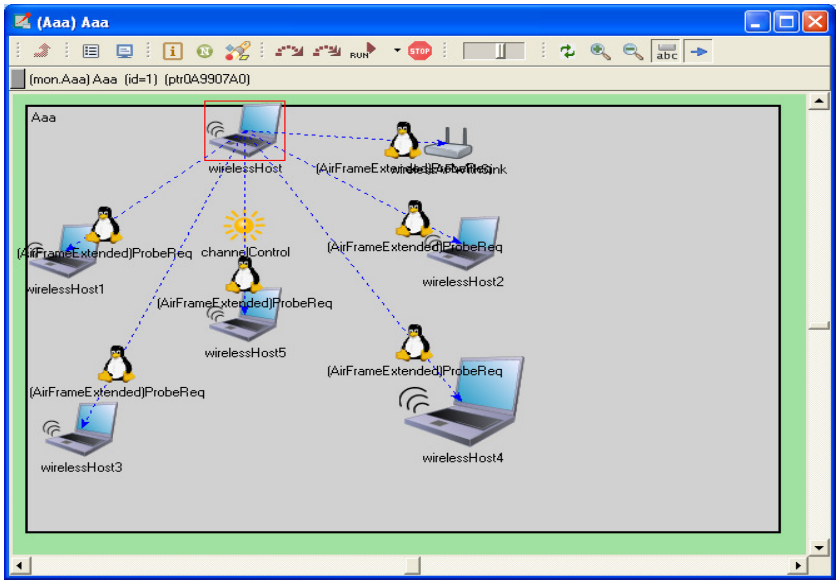

Figure – 4 : Multi hop Routing Simulation in OMNET++

4. MODEL :-

The work is based on Tactical Information Management Middleware architecture proposed in [3] .In these models when the nodes share the MIO (comprising of payload and metadata) during the query to data or data to query communication mode then during this short duration of request - response paradigm the SQL(or TIQL [3]) queries are exchanged. For better management of the query transition between the Source node to Sink Node it is proposed to ex- tends the Tactical Information Management Middleware architecture [3] first by incorporating the concept if In-Network Query Processing [4] and then further strengthening the exchange of the SQL queries it up by suggesting mechanism to handle the SQL injection types of attack. The idea of In-Network Query Processing involves the process of request - response paradigm wherein the multiple SQL or TIQL [3] queries are exchanged between the two mobile nodes who needs to share the data with each other. The queries in Wireless Sensor Network can be classified into following categories [5]:- Our work is based on Tactical Information Management Middleware architecture proposed in [3] . In these models when the nodes share the MIO (comprising of payload and metadata) during the query to data or data to query communication mode then during this short duration of request - response paradigm the SQL(or TIQL [3]) queries are exchanged. For better management of the query transition between the Source node to Sink Node it is proposed to extends the Tactical Information Management Middleware architecture [3] first by incorporating the concept if In-Network Query Processing [4] and then further strengthening the exchange of the SQL queries it up by suggesting mechanism to handle the SQL injection types of attack. The idea of In-Network Query Processing involves the process of request - response paradigm wherein the multiple SQL or TIQL [3] queries are exchanged between the two mobile nodes who

needs to share the data with each other. The queries in Wireless Sensor Network can be classified into following categories [5]:-

1. Monitoring Queries:- The Queries that request the value of one or more attributes continuously and periodically are known as Monitoring queries. Example:- Reporting the status of the no of queries received and queries replied after every 10 seconds.

2. Network Health Queries:- The queries that are concerned with the monitoring the status of the network after regular periodic intervals say after 10 seconds are known as Network Health queries .Example :- The Query for determining the current battery level of the node.

3. Exploratory Queries:- The one-stroke queries that determines the status of a particular node or set of nodes at any given point in time are known as Exploratory queries. These queries generally use the ONCE in the end. Example the query no 9(specified later) can be refined as :- select * from metadata where LocationTimeStamp =’A’ ONCE;

4. Nested Queries :- Many SQL based languages like Tiny DB language does not currently support SQL-style nested queries, because the semantics of such queries are some what ill defined in a streaming environment. Also their exist no clarity that till what level the nesting is allowed to exist in the network.

5. DATABASE SCHEMA

The Database Schema, fig. 5, that is designed to handle these queries comprises of five tables whose DDL(Data Definition Language) is as follows:-

1. Metadata(ID,Description,CTS[CreationTimeStamp], LTS[LocationTimeStamp],Topic)
2. Query[QID, Lifetime, Priority, Rank, AggeragationAllowed,NID[NetworkID])
3. Payload(QueryId,Data)
4. Node(ID,Bandwidth,BatteryPower)
5. Contact(CID[Contact ID],SN[Source Node],DN[Destination Node],ST[Start time],ET[End Time], NCT[Nof times contact has been established],CTDU(Contact Different Time Unit],NID[Node ID)

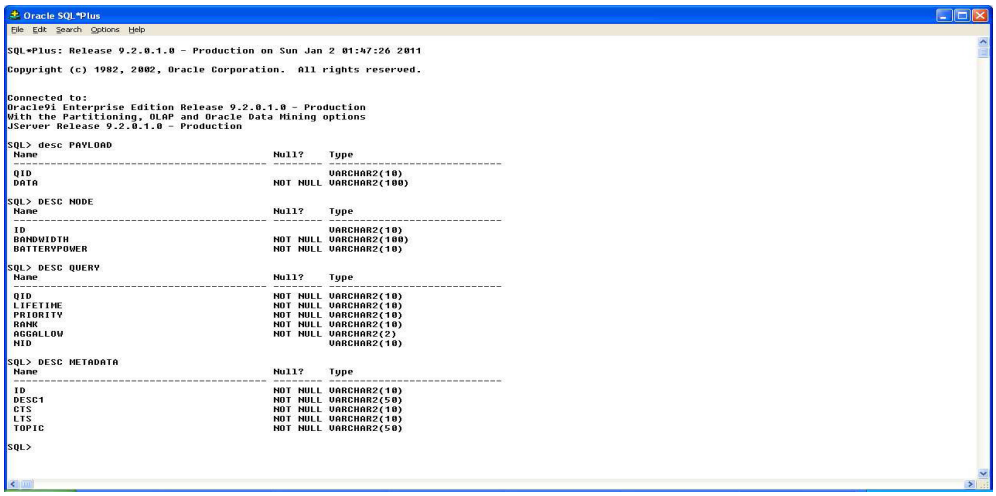

Figure – 5 : ORACLE Snapshot depicting Database Schema

6. SQL CLAUSES

In a DFT-MSN and MP2PN we propose the set of various queries[16,20] which are exchanged between the sensor node and sink node are as follows :-

1. If we want to fetch those queries whose lifetime is greater than 500 seconds and whose rank is more than four then the resultant SQL is :
select _ from query where lifetime <=500 and rank >4;

2. If we want to fetch the information about those nodes whose battery power is greater than 3 milliwatt then the query is as:-
select _ from node where batterypower > `3mw';

3. If we want to fetch all the records from metadata where topic is like document then the SQL Queries is as :-
select _ from metadata where topic like ` document';

4. If we want to fetch all the records from metadata where creation time stamp is greater than 8 am hrs.
select _ from metadata where cts >′ 08 : 00 : 00′;

5. If we want to fetch all the records from query and payload where rank is greater than three then the command is :-
select _ from query, payload where rank > 3 and query.qid=payload.qid

6. If we want to fetch all the records from query where priority is high and the aggregation of the queries is allowed to happen at the sensor node before it is relayed to the sink node :-
select _ from query where priority=` High' and Aggallow=` Y';

7. If we want to fetch all the records from node table where bandwidth is greater than 64 Mb
select _ from node table where Bandwidth > 64;

8. If we want to fetch those records from the table metadata whose LocationTimeStamp is equal to `Zone A'
select * from metadata where LocationTimeStamp =` A';

9. If we want to select the information about those nodes whose start time is greater than 7000 sec but less than 10000 sec.

select * from contact where ST between 7000 and 10000;

10. If we want to select the information about those nodes whose number of contact is greater than 1 and Contact difference is greater than or equal to 1000.

select * from contact where NCT >= 1 AND CTDIFF >= 100

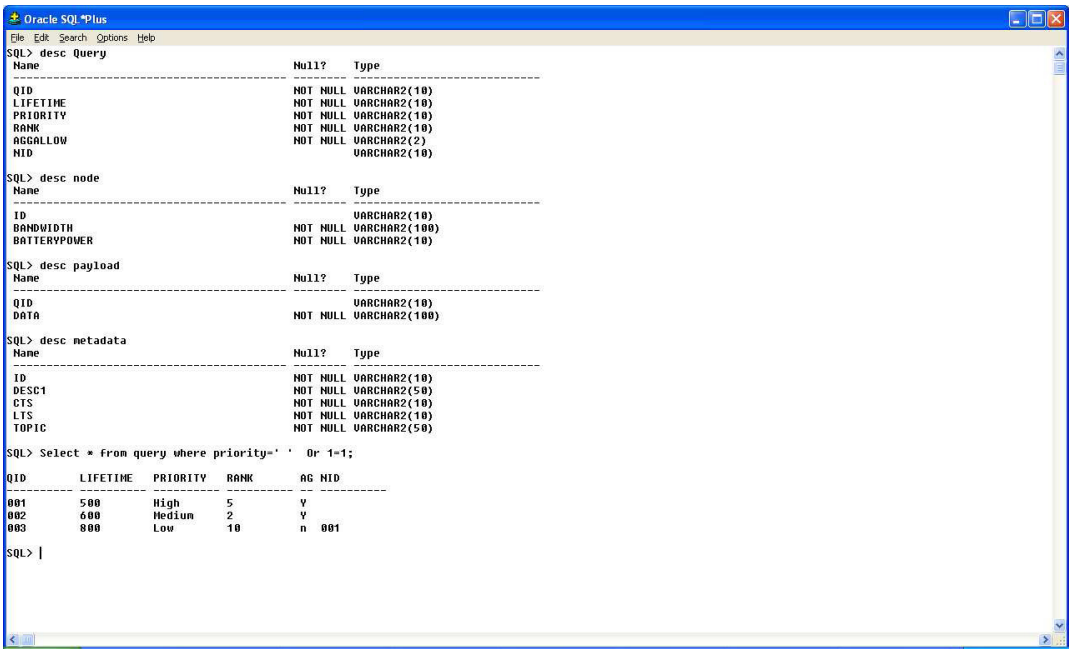

Figure – 6 : ORACLE Snapshot depicting Prospective results of the queries

The result of these queries was obtained once the tables were populated with the data set [Figure 7] obtained during an experiment conducted by the University of Cambridge at the IEEE Infocom 2006 conference in Barcelona [13,21]. Participants included researchers and students, who were asked to carry i-motes with them during the conference and the data on social interactions of the participants was recorded in that duration. In figure 7 , the first column gives the ID of the device who recorded the sightings. The second column gives the ID of the device which was seen. The third and fourth column describe, respectively, the first and last time when the address of ID2 were recorded by ID1 for this contact. The fifth column enumerate contacts with same ID1 and ID2, as 1,2,... . The last column describes the time difference between the beginning of this contact and the end of the previous contact with same ID1 and ID2. It is by convention set to 0 if this is the first contact for this ID1 and ID2.

31	25	240063	240063	13	92635
31	25	240184	240184	14	121
31	25	240527	240527	15	343
31	25	241005	241250	16	478
31	25	250134	250377	17	8884
31	25	250499	250734	18	122
31	25	251905	251905	19	1171
31	25	255080	255080	20	3175
31	25	255330	255330	21	250
31	26	7397	7397	1	0
31	26	7994	7994	2	597
31	26	8002	8117	3	8
31	26	8345	8465	4	228
31	26	9404	9404	5	939
31	26	10348	10348	6	944
31	26	12125	12347	7	1777
31	26	12797	12797	8	450
31	26	142466	142466	9	129669
31	26	142718	142949	10	252
31	26	144370	144370	11	1421
31	26	145798	145798	12	1428
31	26	146036	146160	13	238
31	26	146518	146522	14	358
31	26	148499	148499	15	1977
31	26	176315	176315	16	27816
31	26	177539	178131	17	1224
31	26	182580	182580	18	4449
31	26	182964	182969	19	384
31	26	241005	241250	20	58036
31	26	246436	246436	21	5186
31	26	247838	248319	22	1402
31	27	7876	7876	1	0
31	27	10346	10346	2	2470
31	27	13723	13723	3	3377
31	27	13851	13851	4	128
31	27	13856	14099	5	5
31	27	59248	59365	6	45149
31	27	59725	59732	7	360

Page 1063 of 3994

Figure – 7 : Random Sample Contacts [21]

In this paper an effort is made to discuss and depict by example the different types of the attacks to which the database queries are vulnerable to for instance SQL Injection Attack[7], Denial of Service Attack[ ], Distributed Denial of service Attack[14], Degradation of Service Attack[14] , Query Flood Attack[7,8], Stacked Query Attack[8,9] and suggest some remedial measures how to handle them. Their also exist many number of the open source tools which can be used to detect and handle some of these attacks[16].

7. ATTACKS ON THE SQL QUERIES

7.1 SQL injection attack]7] :- SQL Injection attack is defined as À code injection technique that exploits a security vulnerability occurring in the database layer of an application. The vulnerability is present when user input is either incorrectly filtered for string literal escape characters embedded in SQL statements or user input is not strongly typed and thereby unexpectedly executed [14].

7.2 Query Flood Attack[7,8] :- Query Flood attack can be defined as the typical DoS attack where in the destination node is flooded with infinite no of queries of which only few are genuine coming from the authenticated users and rest of them constituting approx ¾th of the total traffic comes from fake users / malicious nodes with the sole purpose of creating dummy packets so as to clog the network. Majority of these queries are artificial in nature carrying no real request and no real response messages.

7.3 Stacked Query Attack[8,9] :- Stacked query is a term which can be defined to explain the concept that if a database connection layer can handle simultaneous execution of the multiple number of the queries that is it can execute more than one query at a time and each every query is separated by semicolon. However the implementation and the execution of this type of the attack

is very database specific. The following example shows stacked queries in an SQL Injection attack :- SELECT empname FROM employee WHERE id = 1; DROP table employee; DROP table address—

7.4 Degradation-of-service Attack[14] :- The Network is flooded with large number of "Pulsing" or zombies which are nothing but compromised or hacker controlled machines that are remote controlled to launch intermittent ,delay oriented, bursty but non-uniform and short-lived floodings of less/non- secure websites with the intent of merely slowing them down rather than crashing or putting them down. Here the database queries send as part of the http request are hacked , replayed multiple number of times in the network for short intervals so as to create artificial flooding of the queries in the network both to slow down the network as well as to overload the database servers with dummy replayed queries . This type of attack is referred to as "degradation-of-service" attack. In many ways this type of attack is very similar to the Query Flood attack.

7.5 Denial of Service Attack [14] :- Irrespective of the fact how securely an web based application is scripted and carefully compiled , Denial of Service (DoS) attacks always pose a risk. Majority of web applications or web sites are publicly accessible by design, so the server/application really has no way to distinguish millions of authentic user requests from billions of malicious and harmful requests designed to bring it down.

Some common types of DoS attacks which are prevalent on the network are as follows :-

- Consumption of limited pooled resources: for example bandwidth usage, database connections, disk storage, CPU utilization, memory consumption, and interprocess communication and synchronization.
- Attacking resources limited to a particular user, i.e. user lockout or password change
- Troubleshooting the program to cause an unhandled exception, leading to a crash of the application

8. SUGGESTIVE SOLUTIONS TO HANDLE ATTACK :-

Some of the remedial steps which can be initiated to mitigate the attacks are as follows :-

8.1 Degradation of Service and Denial of Service Attacks:-

1. **Monitoring the activities of the Users :-** To make an effort to implement the ITU-T X.800 Security Services Features that includes the steps to ensure that the data confidentiality, data authentication, data access control, data integrity and data availability be maintained so that users must authenticate before they can perform resource-intensive operations (uploads or downloads that consumes huge network bandwidth , complex database queries , frantic changes in the DCL(Data Control language statements such as grant and revoke permissions) to the users by the Database Administrator(DBA) .

2. **Optimization of the database queries** – The database schemas should use the correct data types, the indexes, logical views, efficient stored procedures, securely written cursors and the triggers that activate at the right time to facilitate the execution of the common queries. Query optimization is a quantitative technique, but the basic idea is to ensure you are fully using the features of your database to support application's operations while clearly maintaining the ACID(Atomicity, Concurrency, Isolation and Durability) properties of the real time transactions on the web. A few suggestive tips could be tips be[14]: to avoid usage of

wildcard string queries, to make use of integer/time/date range queries, to use indexed table joins instead of subqueries when possible.

3. **For handling SQL injection attack** :- In order to avoid the SQL injection various measures have been proposed including developing the traditional hashing method for handling the SQL injection but here we focus more on the two techniques as suggested by The Open Web Application Security Project(OWASP) [26] which has proved to be successful methods of mitigating SQL Injection attacks:- a) By developing SQL Queries using bound, typed parameters(b) by writing SQL queries that makes use of parameterized stored procedures. For Example to make SQL Query no 7 SQL injection foolproof the query can be re-written in Java as Select * from query where priority='?' and Aggallow='?'; and the values of priority as high and Aggallow as Yes passed in the two placeholders dynamically at the run time which could provide protection against SQL injection attacks.

9. COMPARITIVE STUDY OF THE ATTACKS IN THE MANET [MOBILE ADHOC NETWORK] AND DFT-MSN AND MP2PN [DELAY/FAULT TOLERANT MOBILE SENSOR NETWORK AND MOBILE PEER TO PEER NETWORK]

S.No	ATTACK NAME	MANET	DFT-MSN AND MP2PN	REASON FOR OCCURENCE OF ATTACKS IN DFT-MSN AND MP2PN
1	SELFISH NODE ATTACK	Yes	No	In the intermittent connected network as the bundles after fragmentation takes multiple path to reach from source to destination therefore it might happen that bundles reach those nodes that are greedy in nature and might start dropping important packets in order to save battery power.
2	BLACKHOLE ATTACK	YES	NO	In the intermittent connected Network the effort is to find the path either through Epidemic Routing technique or through Probabilistic technique to route the packets from source to destination .Here the emphasis is never to find the quick and shortest path as a result the probability of Blackhole attack is highly reduced in the DTN.
3	WORMHOLE ATTACK	YES	YES	The chances of Wormhole attack happening in the Delay Tolerant Network is quite high as here also the intermediate and compromised node can create a tunnel, giving a illusion to the source node that it posses shortest path and might route the packets to reach from source to destination .

4	GRAYHOLE ATTACK	YES	YES	The Chances of the Grayhole attack happening in the DTN is quite high as the compromised nodes can exhibit dual behaviour as at times they can behaves as good node thereby forwarding the bundles as at times exhibit the traits of dropping the bundles resulting in the loss of critical data.
5	SYBIL ATTACK	YES	YES	Sybil attack is usually characterized by the feature that node illegitimately claim multiple identities that is a node can enter into network assuming false/fake identities leading to spoofing in network. The chances of such a attack happening in the network is quite high .
6	COLLABOR ATIVE ATTACK	YES	YES	Yes the Probability of Collaborative attack happening in the DTN is quite high as the cooperative nodes can come under the influence of those nodes that work in tandem with each other and at the same time launch the Grayhole attack and Wormhole attack together.
7	LIFETIME ATTACK OR TTL[TIME TO LIVE] ATTACK	NO	YES	As the time to deliver the packets in DTN can range from minutes to hours, their could be attack where when the value of the TTL field[17] specified in the Lifetime field of the 9^{th} layer of the field format could be proved to be threatening if the intruder attack the delayed or time out packet, change their creation timestamp and put such kind of packets back onto network thereby creating duplicate copies of the already retransmitted packets which results in confusion for the destination that which packet is spoofed one and which one is original.
8	VERSIONIN G ATTACK	NO	YES	Another type of the attack likely to occur in the DTN is the Versioning number attack where in highly skilled intruder can inject into network and change the version no of the bundle being getting transmitted over the Wireless Link which again results in confusion for the destination that which packet is spoofed one and which one is original.

9	CUSTODIA N ATTACK	NO	YES	This type of attack is likely to occur when the hacker or intruder hacks the network and changes the identity of the source field or the custodian(17,18) the intermediate nodes receiving the bundles along the way (and agreeing to accept the reliable delivery responsibility) are called "custodians" of the bundle when the packet is getting transmitted over the network thereby giving false illusion to the destination that the bundle is being getting transmitted from another source. With a result if at all the acknowledgement is being generated by the destination node then it would be transmitted to not the original source but to the hacked or compromised source.
10	PRIORITY DRIVEN ATTACK			This type of attack is likely to occur when priority of the packet is changed during the course of it's transmission from the source to destination. The typical priorities defined are Bulk, Normal and Expedited or express in the range of 1-10 with Bulk having priority in the range of 1-3 , with Bulk having priority in the range of 4-7, with Bulk having priority in the range of 8-10 . If the intruder hacks into network and changes the priority of the packet.

ACKNOWLEDGEMENTS

The author wishes to express sincere thanks to the administration of the GGSIP University and Delhi University for providing the academic environment to pursue the research activities. The author is indebtful to Dr Neelima Gupta, Head Department of Computer Science, University of Delhi for providing valuable guidance in the pursue of this work.

REFERENCES

[1] Yu Wang, Hongyi Wu: Delay/Fault-Tolerant Mobile Sensor Network(DFT-MSN): A new Paradigm for Pervasive Information Gathering. IEEE Trans. Mob. Comput,6(9), 1021–1034 (2007)

[2] Hull, B., Bychkovsky, V., Yang Zhang, Chen, K., Goraczko, M., Shih, E., Balakrish- nan, H., Madden, S.: CarTel: A Distributed Mobile Sensor Computing System. In: 4th International conference on Embedded networked Sensor System, pp. 125–138. ACM, New York (2006)

[3] Bo Xu, Linderman, M., Madria, S., Wolfson, O.: A Tactical Information Manage- ment Middleware for Resource- constrained Mobile P2P Networks. In: 29th IEEE International Symposium on Reliable Distributed Systems, pp. 303–307. New Delhi (2010)

[4] Bo Xu, Vafaee, F., Wolfson, O.: In-Network Query Processing in Mobile P2P atabases. In: 17th ACM SIGSPATIAL International Conferences on Advances in eographic Information Systems, pp. 207–216.ACM, New York (2009).

[5] Madden, S.,R., Franklin, M., J., Hellerstein, J.,M., Wei Hong: TinyDB: An Acqui- sitional Query Processing System for Sensor Networks. ACM Trans.Database Syst.,30(1), 122–173 (2005).

[6] Cerf, V., Hooke, A., Torgerson, L., Durst, R., Scott, K., Burleigh, S., Fall, K., Weiss,H.:RFC 4838, Delay-Tolerant Networking Architecture. IRTF DTN Research Group (2007)

[7] Muhaimin DZulfakar, "Tutorial on Advanced SQL Injection"

[8] Anna Cinnzia Squicciarni, Ivan Paloscia, ElisaBertino,"Protecting Databases from Query Flood Attacks" IEEE(2008).

[9] Natarajan Meghanathan, "Tutorial on Inference Attacks On Sensitive Data and Controls"

[10] http://www.xbow.com/pdf/ Imote2_ press_ release.pdf

[11] http://tools.ietf.org/html/rfc5326

[12] www.servopack.de/support/zebra/ZebraNet-Wireless.pdf

[13] Jain,S., Fall,K., Patra, R.: Routing in Delay Tolerant Network. In: ACM SIGCOMM 04 August 30-September 2004 ,Portland Oregon USA(2004).

[14] http://blogs.captechconsulting.com/blog/daniel-ramsbrock/secure-development-denial-service attacks crawdad.org

[15] http://www.sunspotworld.com

[16] Johari R.,Gupta N., "Insecure Query Processing in Delay/Fault Tolerant Mobile Sensor Network(DFT-MSN) and Mobile Peer to Peer Network" Springer's Communications in Computer and Information Science (CCIS) Series, pp 453-462 July 2011.

[17] http://tools.ietf.org/html/rfc5050

[18] http://tools.ietf.org/html/rfc5326

[19] http://tools.ietf.org/html/rfc4838

[20] Johari R.,Gupta N., Secure Query Processing in Delay Tolerant Network using Java Cryptography Architecture accepted for presentation in IEEE International Conference on Computational Intelligence and Communication Networks (CICN-2011) , October 2011, the proceedings to be published by IEEE Computer Society (CPS) press.

[21] www.crawdad.org

Author

Rahul Johari is working as an Asstt. professor in University School of Information Technology, Delhi, India. He has done his M.Tech in Information Technology from GGSIPU, Delhi. He worked as a Lecturer at Center for the Development of Advanced Computing(C-DAC) NOIDA, from 2004-2007 and as IT consultant from 2001-2003 with C-DAC. His technical and research interests include Advanced Computer Network, SDK Programming, Database Management System, Operating System, Linux and X-Windows Programming, Web Tools and Technologies and OOPS. Presently he is pursuing Ph.D in the domain of Computer Networks from Department of Computer Science, University of Delhi, Delhi.