Scientific Journal of Impact Factor (SJIF): 4.72

e-ISSN (O): 2348-4470
p-ISSN (P): 2348-6406

International Journal of Advance Engineering and Research Development

Volume 4, Issue 4, April -2017

Adaptive and Channel-Aware Detection of Selective Forwarding Attacks in Ad-Hoc Networks

Samira Sayyed, Madhuri Waghule, Rupali Patil

Abstract--- *We propose a Channel-aware name System with adaptive detection threshold (CRS-A) to detect selective forwarding attacks in WSNs. The CRS-A evaluates the info forwarding behaviors of device nodes, in keeping with the deviation of the monitored packet loss and therefore the calculable traditional loss. To optimize the detection accuracy of CRS-A, we tend to on paper derive the best threshold for forwarding analysis, that is accommodative to the time varied channel condition and therefore the calculable attack possibilities of compromised nodes. Moreover, associate attack-tolerant knowledge forwarding theme is developed to collaborate with CRS-A for exciting the forwarding cooperation of compromised nodes and up the info delivery quantitative relation of the network. Intensive simulation results demonstrate that CRS-A will accurately notice selective forwarding attacks and determine the compromised device nodes, whereas the attack-tolerant knowledge forwarding theme will considerably improve the info delivery quantitative relation of the network. We will extend our investigation into wireless circumstantial network with mobile device nodes, wherever the detection of selective forwarding attacks becomes tougher, since the conventional packet loss rate is additional fluctuant and troublesome to estimate attributable to the quality of device nodes.*

Keywords--- *Bloom Filter, CRS-A, Attack-tolerant, WSN, CAD, SCADA.*

1. INTRODUCTION

In some eventualities (e.g., tactical, financial, medical), confidentiality of communicated data between the nodes is necessary; in order that knowledge supposed to (or originated from) a node isn't shared by the other node. Even in eventualities during which confidentiality isn't necessary, it should be dangerous to assume that nodes can continually stay uncompromised. Keeping completely different nodes' data confidential will be viewed as a precaution to avoid a captured node from gaining access to data from alternative uncaptured nodes. Wireless device networks (WSNs) square measure liable to selective forwarding attacks which will maliciously drop a set of forwarding packets to degrade network performance and jeopardize the knowledge integrity. Meanwhile, because of the unstable wireless channel in WSNs, the packet loss rate throughout the communication of device nodes is also high and varies from time to time. It poses an excellent challenge to differentiate the malicious drop and traditional packet loss. During this paper, we have a tendency to propose a Channel-aware name System with adaptive sighting threshold (CRS-A) to detect selective forwarding attacks in WSNs.

The CRS-A evaluates the information forwarding behaviors of device nodes, in line with the deviation of the monitored packet loss and also the calculable traditional loss. To optimize the detection accuracy of CRS-A, we have a tendency to in theory derive the optimum threshold for forwarding analysis, that is adaptive to the time varied channel condition and also the calculable attack possibilities of compromised nodes. What is more, associate attack-tolerant knowledge forwarding theme is developed to collaborate with CRS-A for exciting the forwarding cooperation of compromised nodes and up the information delivery quantitative relation of the network. in depth simulation results demonstrate that CRS-A will accurately sight selective forwarding attacks and determine the compromised device nodes, whereas the attack-tolerant knowledge forwarding theme will considerably improve the information delivery quantitative relation of the network. we are going to extend our investigation into wireless unplanned network with mobile device nodes, wherever the detection of selective forwarding attacks becomes tougher, since the traditional packet loss rate is additional fluctuant and troublesome to estimate because of the quality of device nodes.

In this paper, we have a tendency to think about wireless networks during which messages square measure carried between the supply destination pairs hand and glove in an exceedingly multi-hop fashion via intermediate nodes. in an exceedingly multi-hop network, as information packets square measure transferred, intermediate nodes acquire all or a part of the information through directly forwarding data packets or overhearing the transmission of close nodes. This poses a transparent downside once transferring confidential messages.

We propose a Channel-aware name System with adaptive detection threshold (CRS-A) to detect selective forwarding attacks in WSNs. Specifically, we have a tendency to divide the network period to a sequence of analysis periods. Throughout every analysis amount, device nodes estimate the conventional packet loss rates between themselves and their neighboring nodes, and adopt the calculable packet loss rates to judge the forwarding behaviors of its downstream neighbors on the info forwarding path. The device nodes misbehaving in information forwarding square measure punished with reduced name values by CRS-A. Once the name price of a Senor node is below Associate in nursing alarm price, it'd be known as a compromised node by CRS-A.

2. LITERATURE SURVEY

The literature survey for this project was made by analyzing several top IEEE and other articles from various top journals they are mentioned below.

In paper, **A Survey of Intrusion Detection Systems in Wireless Sensor Networks** by Okan CAN, Ozgur Koray SAHINGOZ, aimed to prepare a survey about intrusion detection systems in wireless sensor networks. Primarily, cyber-attacks occurring in WSNs are described in details. Because of different features (particularly constraints such as energy) of WSNs from wired networks and non-energy constrained wireless networks, IDS in WSN needs different approaches and this approaches are described detailed. Anomalies of WSNs are described and detection techniques of anomaly, misuse (signature based), hybrid detection is pointed out from some studies in recent years.

In the future work, it is aimed to implement this approach in a real WSN system. The necessary learning process can be obtained by using a neural network approach and then can be embedded to the system. Additionally, a key management mechanism can be applied to WSN system to increase the surety of the system.

In paper, **Data-Driven Link Quality Prediction Using Link Features,** TAO LIU and ALBERTO E. CERPA, we studied the usefulness of link quality prediction based on different machine learning methods, such as naive Bayes classifier, logistic regression, and artificial neural networks. Our models take a combination of PRR and PHY information as input, and output the reception probability of the next packe

In paper, **FADE: Forwarding Assessment Based Detection of Collaborative Grey Hole Attacks in WMNs,** Qiang Liu, Jianping Yin, Victor C. M. Leung, Zhiping Cai, we have studied a forwarding assessment based detection scheme, which combines downstream assessments and end-to-end assessments to detect sophisticated selective forwarding attacks. In particular, MRs monitors forwarding behaviours of their downstream nodes via two-hop acknowledgements. By using the monitoring method instead of the classical channel overhearing, the proposed scheme is compatible with security features at the link layer such as those provided by the up-to-date IEEE 802.11 standard. To maximize the detection accuracy, we have carried out theoretical analysis on the optimal detection thresholds under normal losses due to poor channel quality or medium access collisions.

In this paper, **Detection of Malicious Packet Dropping in Wireless Ad Hoc Networks Based on Privacy-Preserving Public Auditing,** Tao shu,Marwan Krunz, we studied that compared with conventional detection algorithms that utilize only the distribution of the number of lost packets, exploiting the correlation between lost packets significantly improves the accuracy in detecting malicious packet drops. Such improvement is especially visible when the number of maliciously dropped packets is comparable with those caused by link errors. To correctly calculate the correlation between lost packets, it is critical to acquire truthful packet-loss information at individual nodes

In paper, **An Integrated Stimulation and Punishment Mechanism for Thwarting Packet Dropping Attack in Multihop Wireless Networks,** Mohamed Elsalih Mahmoud and Xuemin (Sher-man) Shen, they have proposed a novel mechanism that adopts stimulation and punishment strategies to thwart the packet dropping attack in MWNs. Credits are used to stimulate the rational packet droppers to relay the others' packets, and the payment receipts can be processed to detect the broken links to build an RS to identify the irrational packet droppers.

In paper, **Transforming Big Data into Smart Data: Deriving Value via Harnessing Volume, Variety, and Velocity Using Semantic Techniques and Technologies,** Amit P. Sheth ,we studied about Big Data has captured a much of interest in industry, with expectation of better decisions, efficient organizations, and many new jobs. Much of the attention is on the challenges of the four V's of Big Data: Variety, Velocity, Veracity and volume, and methods that control volume, containing storage and computational techniques to support analysis. The concept of Semantic Perception explains how to convert enormous amounts of data into information, meaning, and perception useful for human decision making.

According to study here referred idea to use the concept of Smart Data that is realized by extracting value from a heterogeneous data, and how Smart Data for expanding heterogeneous Big Data authorize a lot of larger class of applications that can profit not just big companies but each individual.

In paper, **Applying Rough Set Technique ,** Jiye Liang, Feng Wang, Chuangyin Dang , about many real data increase dynamically in size. This case takes place in several fields including medical, population studies, and economic research. Since an effective mechanism to deal with such data, cumulative technique has been proposed in the literature.

According to study here referred idea is to use the concept of real data in databases are generated in groups, an effective and efficient group cumulative feature selection algorithm has been proposed which is an extremely important in research of data extraction and knowledge discovery.

In paper, **Combining Big Data Analytics with Business Process using Reengineering,** Meena Jha, Sanjay Jha, Liam O'Brien ,we studied about using data in a myriad new ways to drive business value Big Data can denote different things

to different organizations, but one subject remains constant. Collaboration business process and Big Data analytics using reengineering can deliver the profit to companies and consumers. Big data analytics need to be integrate with business processes to upgrade operations and offer innovative services to customers.
According to study here referred idea is to use the concept of collaboration business process and Big Data analytics using reengineering can provide the profit to companies and consumer.

In paper**, Feature Selection Based on Mutual Information Criteria of Max-Dependency, Max-Relevance and Min-Redundancy,** HanchuanPeng, Fuhui Long, and Chris Ding ,we studied about Feature selection is significant problem for pattern classification system. Making use of minimal-redundancy-maximal-relevance criterion (mRMR), for first-order incremental feature selection later a two-stage feature selection algorithm by collaborating minimal-redundancy-maximal-relevance and other more knowledgeable feature selectors. This permits us to choose a compact set of superior features at very low cost.
According to study mRMR can be effectively combined with other feature selectors such as wrappers to find a very subset from candidate features at lower. Experiments on both distinct and uninterrupted data sets and multiple types of classifiers reveal that the classification accuracy can be notably improved based on mRMR feature selection.

In paper, **Particle Swarm Optimization for Feature Selection in Classification: A Multi-Objective Approach ,** Bing Xue, Mengjie Zhang, Will N. Browne about the Classification problems usually have many features in the data sets, but not all of them are useful. Feature selection intends to choose a small number of admissible features to achieve similar or even better classification performance than using all features. Feature selection algorithms serve the task as a single objective problem.
According to study feature selection intends to choose a small number of admissible features to achieve similar or even better classification performance than using all features.

3. EXISTING SYSTEM

Recent analysis highlighted the key contribution of knowledge in systems wherever the employment of un-trusty data could result in harmful failures (e.g., SCADA systems). Though knowledge modeling, collection, and querying are studied extensively for workflows and curated databases, knowledge in device networks has not been properly addressed. SCADA stands for higher-up management &amp; knowledge Acquisition. SCADA System area unit all open protocol and might be exploited for attacks. A powerfully encrypted, automatic &amp; digitally signed data may be totally different to access even for a legitimate user at a time of crucial deciding. These all needs robust monetary background. The existing works into 2 categories: neighbor police investigation primarily based theme and acknowledgement based. This relies on the various observation techniques for knowledge forwarding.

3.1 Disadvantages of Existing System:

1. As hop-by hop acknowledgement is too tedious and ends in high load.

2. The infected nodes can maliciously drop a subset of forwarding packets to affect the data delivery ratio of the network. It highly impacts data sensitive applications.

3. Traditional security solutions use intensively cryptography and digital signatures, and they employ append-based data structures to store data, leading to prohibitive costs.

4. Existing research employs separate transmission channels for data.

4. PROPOSED SYSTEM

We propose CRS-A, this helps in evaluating the forwarding behaviors of sensor nodes with the help of adaptive detection threshold. An optimal detection threshold to evaluate the forwarding behaviors to optimize the detection accuracy of CRS-A. This optimal threshold is determined for each transmission link in a probabilistic way.

CRS-A is collaborated with a distributed and attack tolerant data forwarding scheme in order to simulate the forwarding cooperation of compromised nodes and improving the data delivery ratio of the network. Instead of removing the compromised nodes from the data forwarding it considers them with time varied channel condition and attack probabilities of neighboring nodes in choosing forwarding nodes.

Proposing DSDV, Destination Sequence Distance Vector algorithm is used to improve the complete network performance in mobile wireless sensor network. The Destination sequence distance vector routing (DSDV) is being derived from the conventional routing information protocol (RIP) for ad-hoc networks routing. It adds an extra sequence number for all the entries in the route table of the conventional RIP. This sequence number helps the mobile nodes to differentiate stale route information from the new and hence prevent the formation of routing loops.

4.1 Advantages of Proposed System:

1. The proposed CRS-A with attack-tolerant data forwarding scheme can achieve a high detection accuracy with both of false and missed detection probabilities close to 0, and improve more than 10% data delivery ratio for the network.
2. Efficient and reliable than existing systems

5. SYSTEM ARCHITECTURE

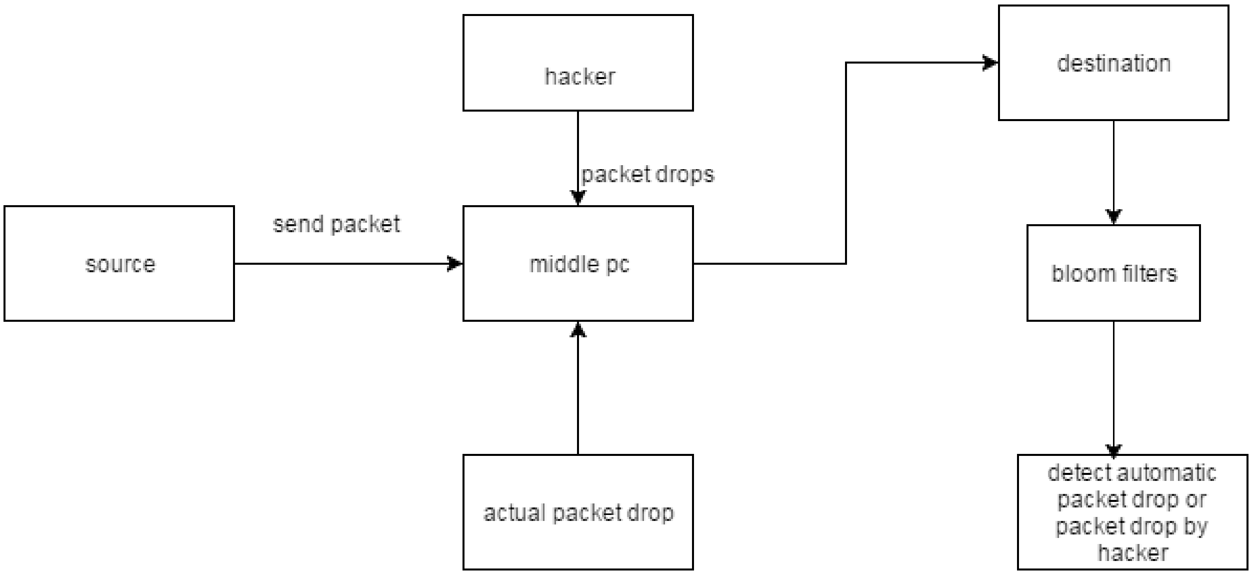


Figure 1. System Architecture of Proposed System

6. MATHEMATICAL MODEL

Let S be the Whole system which consists:
S= {IP, Pro, OP}.
Where,

A. IP is the input of the system.
B. Pro is the procedure applied to the system to process the given input.
C. OP is the output of the system.

A. Input:
IP = {u, F,}.
Where,

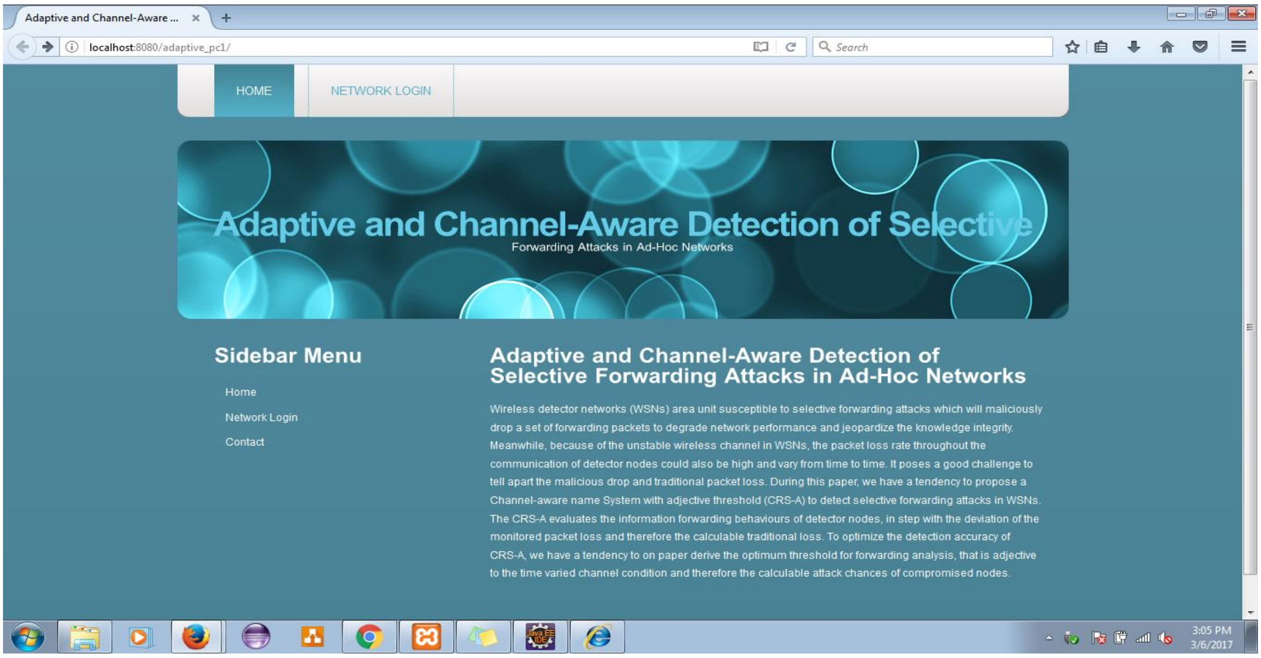
1. u be the user.
2. F be set of files used for sending

B. Process
1. Source node sends packets toward the destination node.
2. At middle pc packet get drop by various factors like low bandwidth, frequency etc.
3. Or any hacker drops/change the packet and forward to destination.
4. At destination detection will be performed whether packet drop by itself or by hacker.

C. Output:
Proper Detection will be done at destination.

7. RESULT ANALYSIS

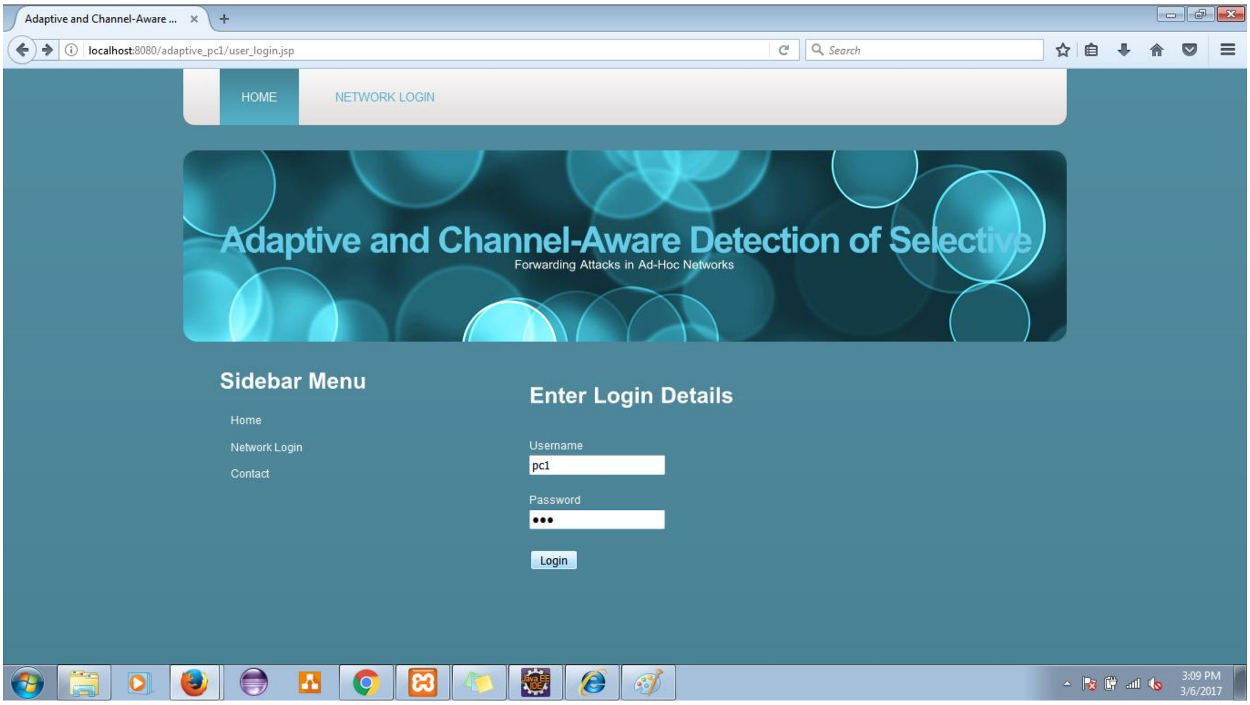
Screenshot 1:


Adaptive and Channel-Aware ...
localhost:8080/adaptive_pc1/
Search
HOME
NETWORK LOGIN
Adaptive and Channel-Aware Detection of Selective
Forwarding Attacks in Ad-Hoc Networks
Sidebar Menu
Home
Network Login
Contact
3:05 PM
3/6/2017

Adaptive and Channel-Aware Detection of Selective Forwarding Attacks in Ad-Hoc Networks

Wireless detector networks (WSNs) area unit susceptible to selective forwarding attacks which will maliciously drop a set of forwarding packets to degrade network performance and jeopardize the knowledge integrity. Meanwhile, because of the unstable wireless channel in WSNs, the packet loss rate throughout the communication of detector nodes could also be high and vary from time to time. It poses a good challenge to tell apart the malicious drop and traditional packet loss. During this paper, we have a tendency to propose a Channel-aware name System with adjective threshold (CRS-A) to detect selective forwarding attacks in WSNs. The CRS-A evaluates the information forwarding behaviours of detector nodes, in step with the deviation of the monitored packet loss and therefore the calculable traditional loss. To optimize the detection accuracy of CRS-A, we have a tendency to on paper derive the optimum threshold for forwarding analysis, that is adjective to the time varied channel condition and therefore the calculable attack chances of compromised nodes.

Screenshot 2:

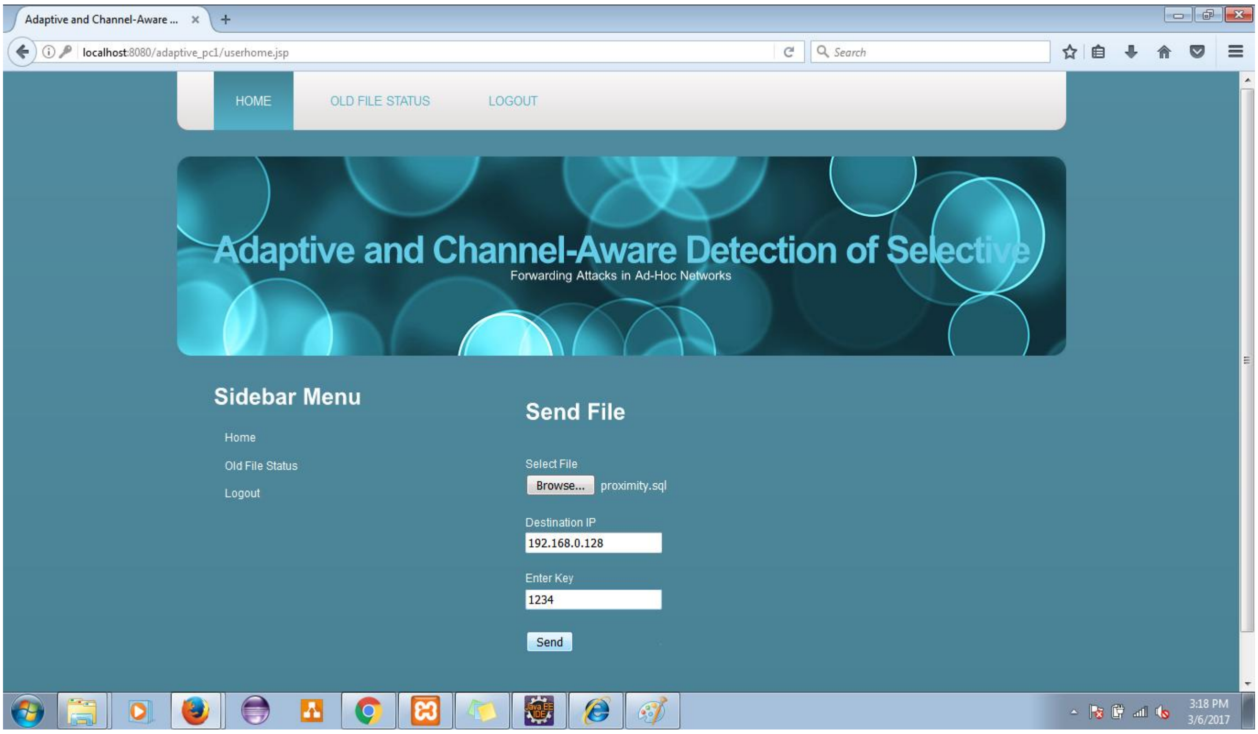

Adaptive and Channel-Aware ...
localhost:8080/adaptive_pc1/user_login.jsp
Search
HOME
NETWORK LOGIN
Adaptive and Channel-Aware Detection of Selective
Forwarding Attacks in Ad-Hoc Networks
Sidebar Menu
Home
Network Login
Contact
Login
3:09 PM
3/6/2017

Enter Login Details

Username: pc1

Password: •••

Screenshot 3:


Adaptive and Channel-Aware ...
localhost:8080/adaptive_pc1/userhome.jsp
Search
HOME
OLD FILE STATUS
LOGOUT
Adaptive and Channel-Aware Detection of Selective
Forwarding Attacks in Ad-Hoc Networks
Sidebar Menu
Home
Old File Status
Logout
Browse...
Send
3:18 PM
3/6/2017

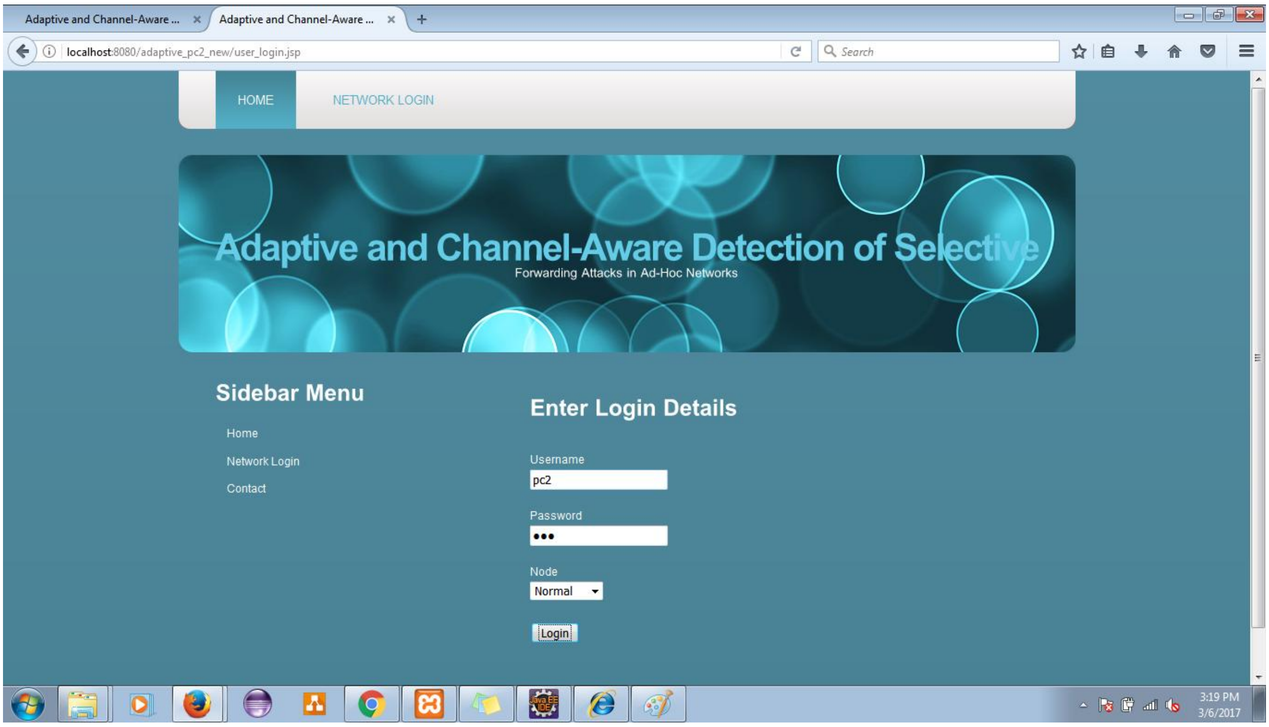
Send File

Select File: proximity.sql

Destination IP: 192.168.0.128

Enter Key: 1234

Screenshot 4:


Adaptive and Channel-Aware ...
Adaptive and Channel-Aware ...
localhost:8080/adaptive_pc2_new/user_login.jsp
Search
HOME
NETWORK LOGIN
Adaptive and Channel-Aware Detection of Selective
Forwarding Attacks in Ad-Hoc Networks
Sidebar Menu
Home
Network Login
Contact
Login
3:19 PM
3/6/2017

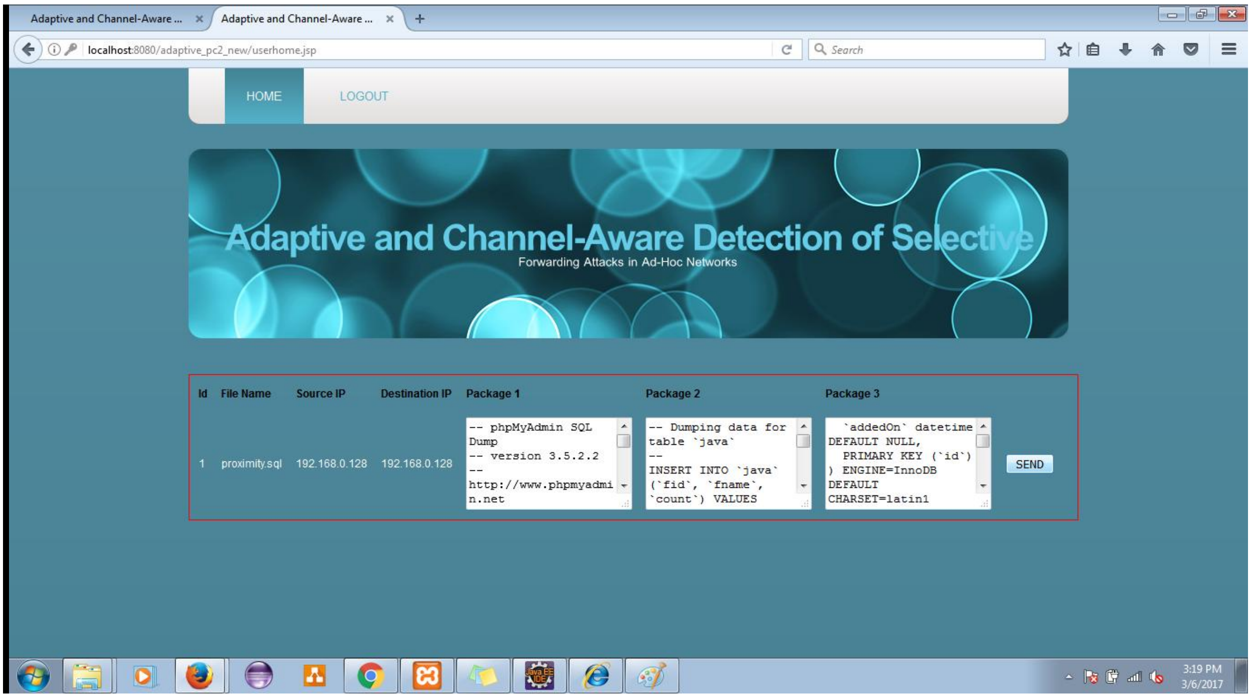
Enter Login Details

Username: pc2

Password: •••

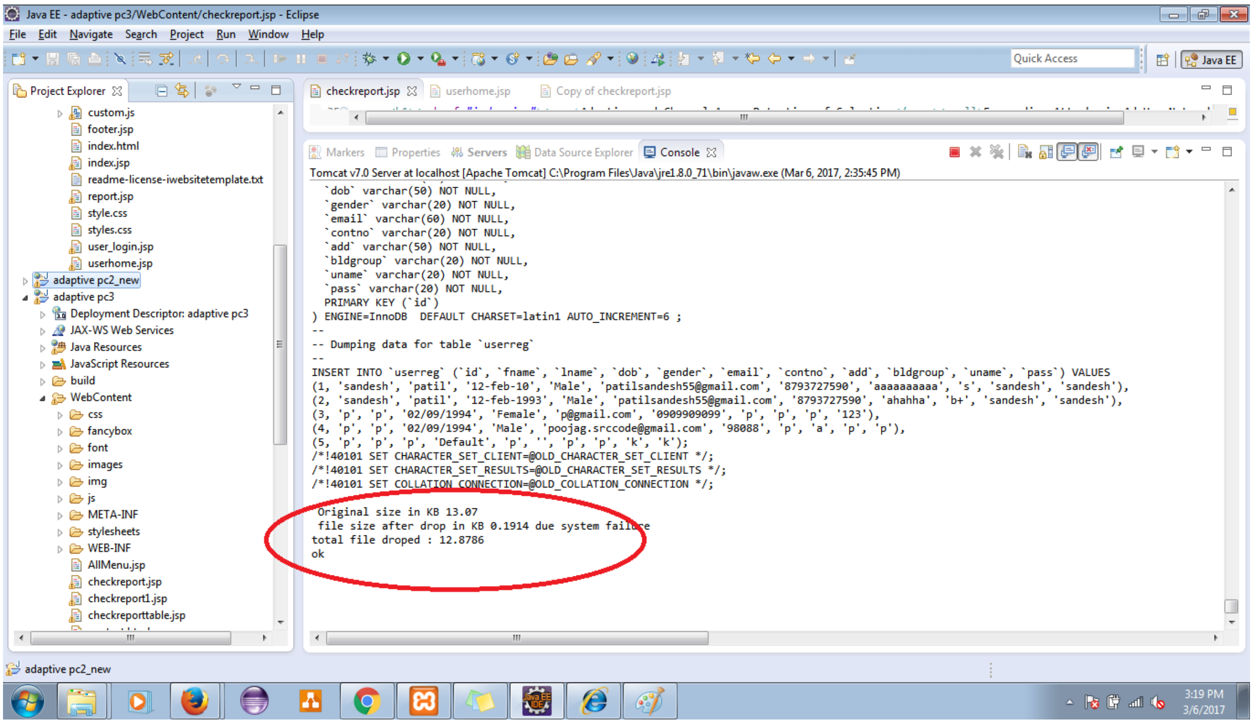
Node: Normal

Screenshot 5:


Adaptive and Channel-Aware ...
Adaptive and Channel-Aware ...
localhost:8080/adaptive_pc2_new/userhome.jsp
Search
HOME
LOGOUT
Adaptive and Channel-Aware Detection of Selective
Forwarding Attacks in Ad-Hoc Networks
3:19 PM
3/6/2017

Id	File Name	Source IP	Destination IP	Package 1	Package 2	Package 3	
1	proximity.sql	192.168.0.128	192.168.0.128	-- phpMyAdmin SQL Dump -- version 3.5.2.2 -- http://www.phpmyadmin.net	-- Dumping data for table `java` -- INSERT INTO `java` (`fid`, `fname`, `count`) VALUES	`addedOn` datetime DEFAULT NULL, PRIMARY KEY (`id`)) ENGINE=InnoDB DEFAULT CHARSET=latin1	SEND

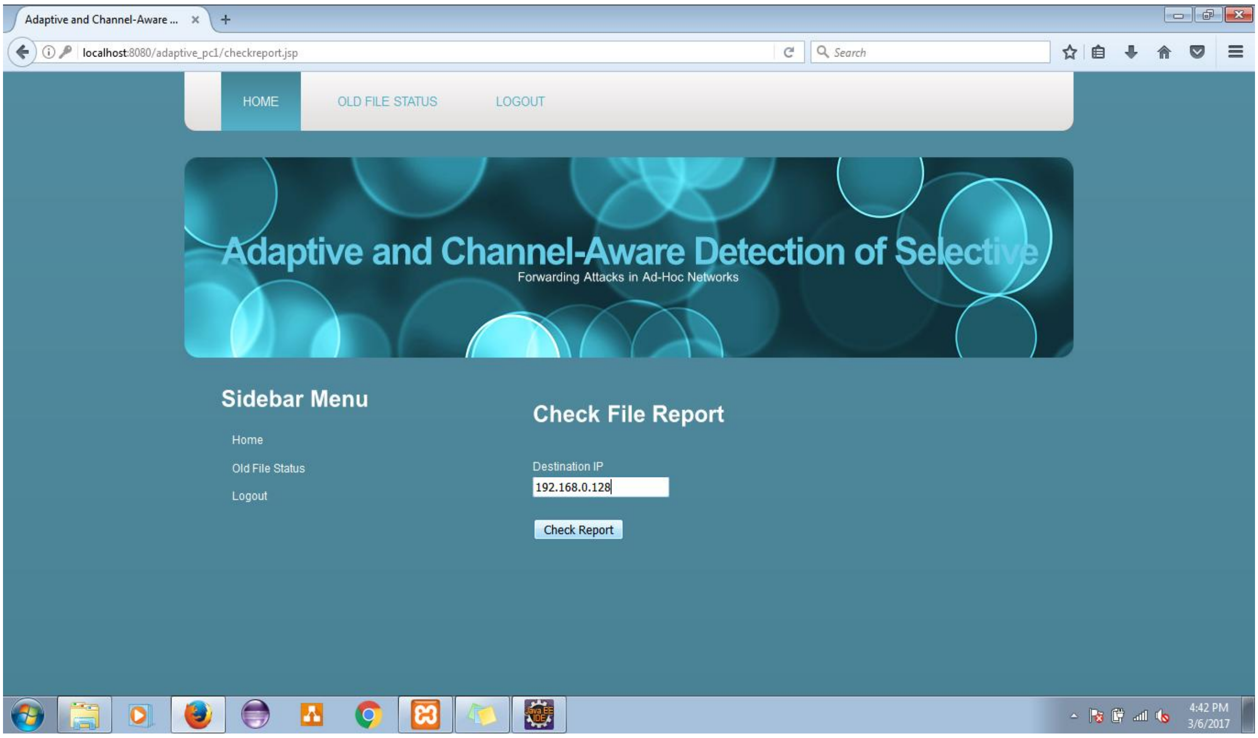
Screenshot 6:



```
Tomcat v7.0 Server at localhost [Apache Tomcat] C:\Program Files\Java\jre1.8.0_71\bin\javaw.exe (Mar 6, 2017, 2:35:45 PM)
  `dob` varchar(50) NOT NULL,
  `gender` varchar(20) NOT NULL,
  `email` varchar(60) NOT NULL,
  `contno` varchar(20) NOT NULL,
  `add` varchar(50) NOT NULL,
  `bldgroup` varchar(20) NOT NULL,
  `uname` varchar(20) NOT NULL,
  `pass` varchar(20) NOT NULL,
  PRIMARY KEY (`id`)
) ENGINE=InnoDB  DEFAULT CHARSET=latin1 AUTO_INCREMENT=6 ;
--
-- Dumping data for table `userreg`
--
INSERT INTO `userreg` (`id`, `fname`, `lname`, `dob`, `gender`, `email`, `contno`, `add`, `bldgroup`, `uname`, `pass`) VALUES
(1, 'sandesh', 'patil', '12-feb-10', 'Male', 'patilsandesh55@gmail.com', '8793727590', 'aaaaaaaaaa', 's', 'sandesh', 'sandesh'),
(2, 'sandesh', 'patil', '12-feb-1993', 'Male', 'patilsandesh55@gmail.com', '8793727590', 'ahahha', 'b+', 'sandesh', 'sandesh'),
(3, 'p', 'p', '02/09/1994', 'Female', 'p@gmail.com', '0909909099', 'p', 'p', 'p', '123'),
(4, 'p', 'p', '02/09/1994', 'Male', 'poojag.srccode@gmail.com', '98088', 'p', 'a', 'p', 'p'),
(5, 'p', 'p', 'p', 'Default', 'p', '', 'p', 'p', 'k', 'k');
/*!40101 SET CHARACTER_SET_CLIENT=@OLD_CHARACTER_SET_CLIENT */;
/*!40101 SET CHARACTER_SET_RESULTS=@OLD_CHARACTER_SET_RESULTS */;
/*!40101 SET COLLATION_CONNECTION=@OLD_COLLATION_CONNECTION */;

 Original size in KB 13.07
 file size after drop in KB 0.1914 due system failure
total file droped : 12.8786
ok
```

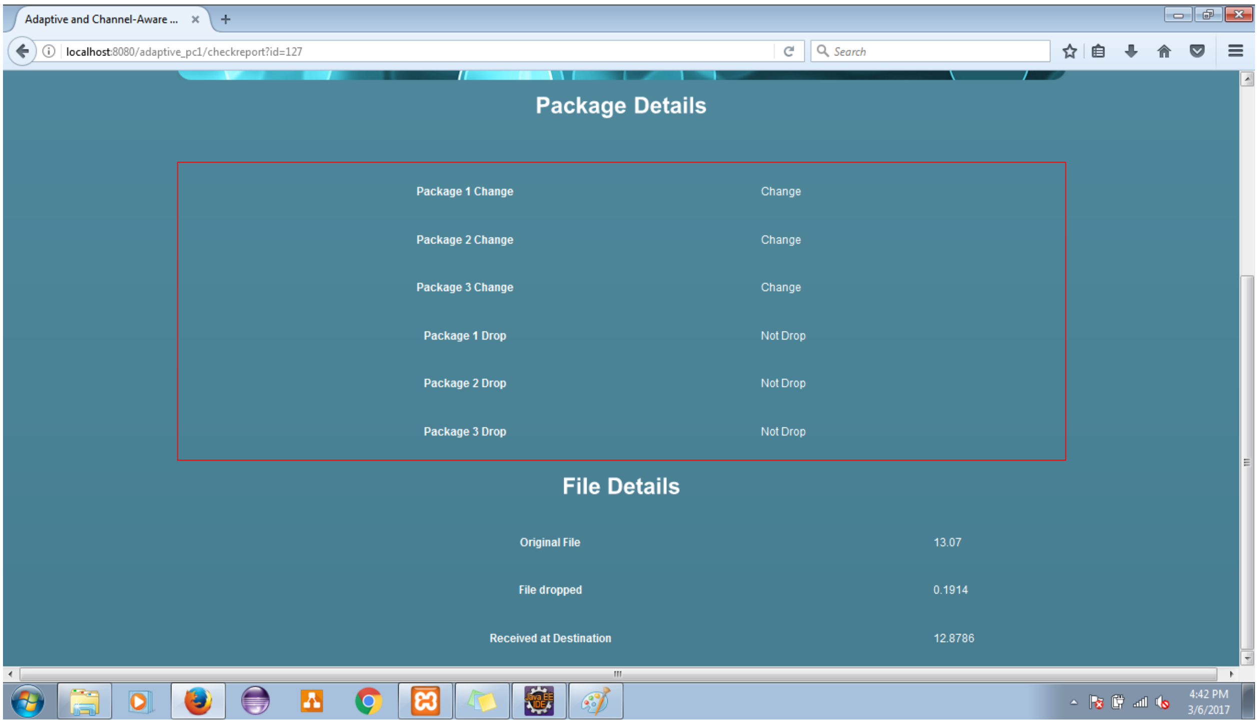
Screenshot 7:


Adaptive and Channel-Aware ...
localhost:8080/adaptive_pc1/checkreport.jsp
Search
HOME
OLD FILE STATUS
LOGOUT
Adaptive and Channel-Aware Detection of Selective
Forwarding Attacks in Ad-Hoc Networks
Sidebar Menu
Home
Old File Status
Logout
Check Report
4:42 PM
3/6/2017

Check File Report

Destination IP: 192.168.0.128

Screenshot 8:


Adaptive and Channel-Aware ...
localhost:8080/adaptive_pc1/checkreport?id=127
Search
4:42 PM
3/6/2017

Package Details

Package 1 Change	Change
Package 2 Change	Change
Package 3 Change	Change
Package 1 Drop	Not Drop
Package 2 Drop	Not Drop
Package 3 Drop	Not Drop

File Details

Original File	13.07
File dropped	0.1914
Received at Destination	12.8786

8. CONCLUSION

In this paper, we considered the problem of resource allocation in wireless multi-hop networks where sources have confidential information to be transmitted to their corresponding destinations with the help of intermediate nodes over time-varying uplink channels. All intermediate nodes are considered as internal eavesdroppers from which the confidential information needs to be protected. To provide confidentiality in such setting, we propose encoding the message over long blocks of information which are transmitted over different paths.

9. REFERENCES

[1] L. Georgiadis, M. J. Neely, and L. Tassiulas, "Resouce allocation and cross-layer control in wireless networks," *Found. Trends Netw.*, vol. 1,no. 1, pp. 1–144, 2006.

[2] X. Lin, N. B. Shroff, and R. Srikant, "On the connection-level stability of congestion-controlled communication networks," *IEEE Trans. Inf.Theory*, vol. 54, no. 5, pp. 2317–2338, May 2008.

[3] P. K. Gopala, L. Lai, and H. E. Gamal, "On the secrecy capacity of fading channels," *IEEE Trans. Inf. Theory*, vol. 54, no. 10, pp. 4687–4698, Oct. 2008.

[4] A. Khisti and G. W. Wornel, "Secure transmissions with multiple antennas:The misome wiretap channel," *IEEE Trans. Inf. Theory*, vol. 56, no. 7, pp. 3088–3014, July 2010.

[5]L. Dong, Z. Han, A. P. Petropulu, and H. V. Poor, "Improving wireless physical layer security via cooperating relays," *IEEE Trans. Signal Process.*, vol. 58, no. 3, pp. 4033–4039, Mar. 2010.

[6]O. O. Koyluoglu, C. E. Koksal, and H. E. Gamal, "On secrecy capacity scaling in wireless networks," *IEEE Trans. Inf. Theory*, vol. 58, no. 5, pp. 3000–3015, May 2012.

[7]C. Capar, D. Goeckel, B. Liu, and D. Towsley, "Secret communication in large wireless networks without eavesdropper location information," in *Proc. IEEE INFOCOM*, Orlando, FL, USA, Mar. 2012,pp. 1152–1160.

[8]N. Cai and R. Yeung, "Secure network coding," presented at the 2002 IEEE Int. Symp. Inf. Theory, Lausanne, Switzerland, Jun. 2002.