Process Calculi for Intrusion Detection System in Mobile Ad-hoc Networks

Parul Yadav[1] and Manish Gaur[2]
[1] Institute of Engineering & Technology, Lucknow, U.P., 226021, India
[2] Centre for Advanced Studies, Lucknow, U.P., 226021, India
Email: parul.pec@gmail.com; manish.gaur@ietlucknow.ac.in

Abstract —Security of routing protocols is one of the crucial and emerging issues in Mobile Ad-hoc Networks. A lot of secure versions of routing protocols in Mobile Ad-hoc Networks have already been proposed by eminent researchers. But most of them are tested by means of simulation. Simulation techniques have their limitations as they can only find presence of error rather than absence of error. To overcome this situation, formal methods are used that can verify systems using theorem proving or automated model checking techniques. We are the first who propose a calculi for Intrusion Detection System (IDS) to secure routing in Mobile Ad-hoc Networks in a process algebraic framework. The proposed calculi is basically an extension of distributed pi calculus (Dpi). The novelty of the proposed calculi is to model stand-alone IDS covering both network & host-based IDSs. The calculi has two syntactic categories: one for nodes and another for processes. We justify our model by providing its reduction equivalence, after abstracting away the details of IDS (implementation), to its specification calculus for energy-aware broadcast, unicast and multicast communications of MANETs (E-BUM). We believe that such modelling helps in detecting intrusion(s) in Mobile Ad-hoc Networks and that in turn will provide secure and energy efficient route.

Index Terms—Process algebra for IDS, calculus for intrusion detection system in MANETs, formal framework for security in MANETs

I. Introduction

Mobile Ad-hoc Network, an ultimate dimension of wireless networks, is an arbitrary collection of independent nodes that can form or deform the network on the fly without any administration or infrastructure [1]-[3]. Mobile ad-hoc network allows nodes to communicate with each other via radio transceivers that have limited radio transmission range. Highly dynamic topology and infrastructure-less architecture of MANETs make these innovative networks vulnerable to various security attacks [4]. In Mobile Ad-hoc Networks, security attacks can be classified according to their origin or their nature. Based on the origin, attacks are divided into two categories, external and internal [4]. On the basis of operation of the network, attacks in mobile ad-hoc networks are categorized as active and passive attack. Besides it, routing attacks are also classified into five categories: attacks using impersonation, modification, fabrication, replay, and Denial of Service (DoS). Thus security of routing protocols for mobile ad-hoc networks is an active area of research [4].

The challenge of MANETs is to design and verify robust routing protocol with adequate security schemes for these innovative networks. Various secure routing protocols have already been proposed in [5]-[10]. Most of these, verified using simulation tools [11], still have flaws. The simulation-tools have certain limitations like scenario specific results, limited scalability etc.. Thus, simulation tool [12] can not be used to verify these systems by exploring all conditions related to them. On the other hand, using formal methods, these systems can be modelled, and then verified using theorem prover or (semi) automated model checking techniques. Researchers in [13]-[17] provide formal frameworks to model basic properties like node mobility, local broadcast and dynamic topology etc. of MANETs and attack prevention technique like public key cryptography mechanism for secure routing in MANETs. Attack prevention techniques, a first line of defence, such as encryption, key management and authentication can prevent the network from a set of known attacks. Thus, in addition to prevention, second line of defence called as detection and response is also required to deploy layered security mechanism. One of the such detection and response systems is called as Intrusion Detection System [18].

The objective of this research paper is to model an Intrusion Detection System for secure routing in MANETs [3] in a process algebraic framework [19]. This detection model will detect intrusion(s) in MANETs that will result in providing secure route. Our proposed model or calculi will also ensure energy efficient route [3]. We intend to extend Distributed pi calculus for modelling MANET.

In our proposed calculi named as dRi , a system term will have an evolution like $\Gamma_c \rhd S \rightarrow \Gamma_c \rhd S'$ where $\Gamma_c \rhd S$ is a well-formed configuration, S is a system term and S' is its reduced form after the reduction taken place. System term S can be typically of the form $\langle I^{\alpha}, D \rangle n[P]_r^{\ell}$ with network address n , physical location ℓ , transmission radius r and process P , data

Manuscript received April 20, 2018; revised October 8, 2018.
Corresponding author email: parul.pec@gmail.com.
doi:10.12720/jcm.13.11.635-647

store D and various internal components α of IDS I. This will empower us to model intrusion detection system in MANETs. This system is an elaboration of calculus for energy-aware broadcast, unicast and multicast communications of MANETs (E-BUM) [19]. We justify this model by showing the reduction equivalence of $\Gamma \triangleright S$ to R, where R is a system term in E-BUM [19].

This paper is organized in five sections. Section 2 and 3 brief key features, syntax, structural equivalence and reduction semantics of *dRi*. In section 4, we present an example to elaborate more about the proposed model *dRi*. Section 5 presents reduction equivalence of *dRi* with its specification [19]. Section 5 is the conclusion. Proposed process calculi for the detection model, named as *dRi* is given in the next section.

II. Proposed Calculi

Mobile Ad-hoc Network consists of collection of mobile nodes. A small mobile ad-hoc network having nodes A, B, C,....., H is shown in Fig. 1. A network, shown in Fig. 1, depicts transmission range of node A, communication links and data store at nodes. Fig. 1 depicts that node B, C, D and E are in transmission range of node A. Each node can be characterized by its features like its transmission range, network address & physical location and possess executing process or running code & data store on it. The features of a node in MANETs, are shown in Fig. 2. These networks are highly vulnerable to security attacks and may disturb routing in MANETs. To ensure secure routing in MANETs, we modelled stand alone Intrusion Detection System (IDS). Stand- alone IDS can be conceptually structured into four internal components: the data collection module, the feature extraction module, the local detection engine and the local response module as shown in Fig. 3. Our proposed calculi, named as *dRi*, models IDS in MANETS. Major key features of *dRi* are as follow:

- In *dRi*, syntax for node covers its network address, physical location, transmission radius and executing processes.
- It models dynamic topology using distance function. It will incorporate node mobility when it moves in or out from its transmission range and node failure up to some extent.
- It ensures energy efficiency by adjusting transmission power of node.
- It supports unicast, multicast, broadcast transmissions.
- It models stand-alone IDS covering both network and host-based IDSs.
- It defines detection model to detect external and internal attackers. Detection model abstracts mathematical analysis for actions of nodes in order to find any undesirable activity in the network.

Syntax and structural equivalence for our proposed calculi *dRi* are given in next subsections.

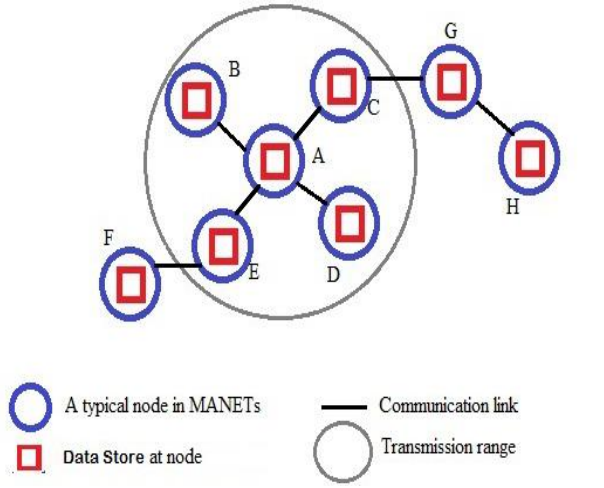

Fig. 1. A mobile ad-hoc network

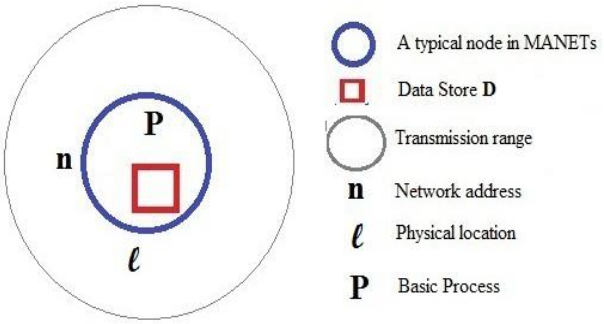

Fig. 2. A typical node in mobile ad-hoc network

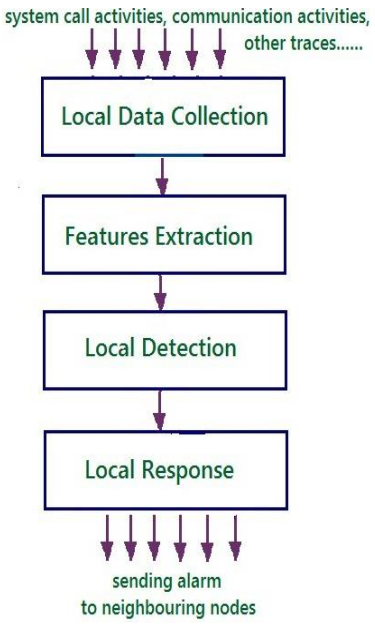

Fig. 3. A conceptual intrusion detection model

A. Syntax

There are two syntactic categories in *dRi*. First syntactic category is for nodes forming a network. Second syntactic category is for processes residing at each node. The calculi *dRi* has system terms, named as $M_1, M_2, \ldots\ldots$. A system term consists of a collection of nodes $n_1, n_2, \ldots\ldots$. A basic syntax of a node is defined

as $\langle I^{\alpha}, D\rangle n[P]_r^{\ell}$ where, I denotes IDS that is capable enough to manage data store D and all four internal components α of IDS I. The syntax for this code is a straightforward instance of a standard process calculus. The syntax of the nodes and processes are given in Fig. 4. The intuitive meaning of each of the syntactic constructs given in Fig. 4 is as follows:

Nodes

M	::=	ϵ	Empty network
	|	$M_1 \mid M_2$	Parallel composition
	|	$\langle I^{\alpha}, D\rangle n[P]_r^{\ell}$	Node

Processes

P	::=	$stop$	Termination
	|	$c! < \tilde{\nu}, \tilde{n} >$	Output
	|	$c?(\tilde{x}, \tilde{y})P$	Input
	|	$if\ b\ then\ P_1\ else\ P_2$	Matching
	|	$P_1 \mid P_2$	Parallel composition
	|	$*P$	Recursion

Fig. 4. Syntax for nodes and processes

Nodes

- Empty network which has no node, is represented by the term ε.
- $M_1 \mid M_2$ represents two networks working in parallel.
- $\langle I^{\alpha}, D\rangle n[P]_r^{\ell}$ represents node where, process P can participate in both inter node communication and intra node communication. Intra node communication, that is a communication within a node, helps to implement IDS at each node.

Processes

- The simplest possible process, which does nothing, is represented by the term $stop$.
- The term $c!< \hat{v}, \tilde{n} >$ represents the next simplest process, which first evaluates a closed expression $\hat{v}$ to some value $\tilde{v}$ and then transmits the value $\tilde{v}$ and list of receivers $\tilde{n}$ along the channel c. Channel c is used for inter node communication or intra node communication. Forms of $\hat{v}$ can be represented using a ternary set defined by $\{0,1,\tilde{v}\}$ where 0 and 1 indicates that node under consideration is non-malicious node and malicious node respectively and $\tilde{v}$ donates broadcast message other than alarm message. List of receivers $\tilde{n}$ ranges over n_1, n_2 ,.....,. where $\tilde{n}$ can be singleton or finite set to represent unicast or multicast communication respectively. $\tilde{n} = \infty$ indicates broadcast communication. Possible forms for output process and their respective meaning are given in Table I.

TABLE I: POSSIBLE FORMS FOR $c! < \hat{\nu}, \tilde{n} >$ AND THEIR RESPECTIVE MEANING

Forms for $c! < \hat{\nu}, \tilde{n} >$	Meaning
$c! < 1, n >$	Node n is dectected to be a malicious node and this alarm message needs to broadcast to all nodes in the network.
$c! < 0, n >$	Node n is not found to be a malicious node. This form can be obtained as an output of Local Dectection Module of IDS.
$c! < \tilde{v}, n >$	$[\hat{\nu}] = \tilde{v} \neq 0$ or 1, unicast the value $\tilde{v}$ for destination node with network address n along the channel c.
$c! < \tilde{v}, \tilde{n} >$	$[\hat{\nu}] = \tilde{v} \neq 0$ or 1, multicast the value $\tilde{v}$ for destination nodes with network address in $\tilde{n}$ along the channel c.
$c! < \tilde{v}, \infty >$	$[\hat{\nu}] = \tilde{v} \neq 0$ or 1, braodcast the value $\tilde{v}$ to all nodes in the network along the channel c.

- Input from a channel c is represented by the term $c?(\tilde{x}, \tilde{y})P$ where, forms of $\tilde{x}$ & $\tilde{v}$ and $\tilde{y}$ & $\tilde{n}$ must match. The process $c?(\tilde{x}, \tilde{y})P$ may input a value $\tilde{v}$ and list of receivers $\tilde{n}$ along the channel c, deconstruct it using the pattern $\tilde{x}$ and $\tilde{y}$ and then execute P into which the components of $\tilde{v}$ and $\tilde{n}$ have been substituted, which we will denote by $P\{\tilde{v}/\tilde{x}, \tilde{n}/\tilde{y}\}$.
- $if\ b\ then\ P_1\ else\ P_2$ is a test using boolean expression returning value either $true$ or $false$.
- $P_1 \mid P_2$ represents two processes running in parallel.
- $*P$ represents recursive process.

Now we discuss configuration of system in dRi.

Definition: (Configuration) A configuration is a pair $\Gamma_c \triangleright M$ where, Γ_c is an environment holding network connectivity function and M is/are system term(s) as defined in Fig. 4. Network connectivity function exhibits connectivity among network nodes. Γ_c defined as $\Gamma_c : N \mapsto N$ has finite domain and co-domain where N is set of node names or network addresses $(n_1, n_2, n_3, ...)$. Suppose M_1 defined as $\langle I^{\alpha}, D_1\rangle n_1[P_1]_{r_1}^{\ell_1}$ and M_2 defined as $\langle I^{\alpha}, D_2\rangle n_2[P_2]_{r_2}^{\ell_2}$ are two system terms or nodes. There are 2 possible notations to represent connectivity between n_1 and n_2.

1. *Connected:* In dRi, connectivity function $\Gamma_c \bullet\!\!\mapsto n_1(\ell_1..\ell_1')(r_1..r_1') \uparrow n_2(\ell_2..\ell_2')(r_2..r_2')$ implies $\Gamma_c \bullet\!\!\mapsto n_1 \uparrow n_2$ defines that n_1 can participate in communication with n_2. Node n_1 and n_2 can move from physical locations ℓ_1 and ℓ_2 to ℓ_1' and ℓ_2' respectively in one computational step such that $d(\ell_1, \ell_1') \leq \delta$ and $d(\ell_2, \ell_2') \leq \delta$. Here communication is unidirectional where, n_1 can broadcast the message and n_2 can directly receive well-formed message on common communication channel.

2. *Disconnected:* In *dRi* , connectivity function $\Gamma_c \bullet\!\!\mapsto n_1(\ell_1..\ell'_1)(r_1..r'_1) \downarrow n_2(\ell_2..\ell'_2)(r_2..r'_2)$ implies $\Gamma_c \bullet\!\!\mapsto n_1 \downarrow n_2$ defines that n_2 can not directly receive message sent by n_1 . There is not any unidirectional communication link from n_1 to n_2 . Thus node n_1 can not directly participate in communication with n_2 .

Properties of Connectivity Function Γ_c

1. Γ_c defined as $\Gamma_c : N \mapsto N$ has finite domain and codomain where N is set of node names or network addresses $(n_1, n_2, n_3,.....)$.

2. $\Gamma_c \bullet\!\!\mapsto n_1 \uparrow n_2$ is well-formed iff $n_1 \neq n_2$. It ensures that message sent by a node can not be received by the same node. This rule checks self loop formation in network graph formed using network connectivity function.

3. $\Gamma_c \triangleright \langle I^\alpha, D\rangle n[P_1]^\ell_r \mid \Gamma_c \triangleright \langle I^\alpha, D\rangle n[P_2]^\ell_r$ implies $\Gamma_c \triangleright \langle I^\alpha, D\rangle n[P_1 \mid P_2]^\ell_r$

The configuration $\Gamma_c \triangleright M$ is a well-formed configuration if:

1. $nodes(M) \subseteq \Gamma_c$; models that connectivity function has information of every node in the network.

2. for any node(s) n_1 and n_2, if $\Gamma_c \bullet\!\!\mapsto n_1 \uparrow n_2$, then $n_1 \neq n_2$; corresponds that node can not listen its own transmission that in terns ensures self-loop free connectivity.

3. $M \varepsilon ISys$; indicates that each node in a system term can have only one code for all four components of IDS.

Structural Equivalence for *dRi* is given in next subsection.

B. Structural Equivalence

We use a equivalence relation $\equiv$ between the systems and processes, called as structural equivalence. Structural equivalence $\equiv$ is defined for each syntactic categories. Structural equivalence $\equiv$ represents the systems and processes as same computational entities. Structural equivalence in *dRi* is defined in Fig. 5. Reduction Semantics in *dRi* that relies on relation, structural equivalence $\equiv$ is given in next section.

Structural Equivalence (System)

(M-COM)	$M_1 \mid M_2$	$\equiv M_2 \mid M_1$
(M-STOP)	$M \mid \epsilon$	$\equiv M$
(M-ASSOC)	$(M_1 \mid M_2) \mid M_3$	$\equiv M_1 (M_2 \mid M_3)$

Structural Equivalence (Process)

(P-COM)	$P_1 \mid P_2$	$\equiv P_2 \mid P_1$
(P-ASSOC)	$(P_1 \mid P_2) \mid P_3$	$\equiv P_1 \mid (P_2 \mid P_3)$
(P-STOP)	$P \mid stop$	$\equiv P$

Structural Equivalence (Process:System)

(M-EQ) $\dfrac{P_1 \equiv P_2}{\langle I^\alpha, D\rangle n[\![P_1]\!]^\ell_r \equiv \langle I^\alpha, D\rangle n[\![P_2]\!]^\ell_r}$

Fig. 5. Structural equivalence

(R-*dRi*-e-COMM)

$$\frac{\forall i \epsilon I,\ \Gamma_c \vdash n \uparrow n_i, d(\ell, \ell') \leq \delta,\ d(\ell_i, \ell'_i) \leq \delta,\ n \neq n_i,\ \alpha \epsilon \{e, a\},\ \neg rec(M_f, c)\ \forall n' \epsilon\ nodes(M_{\not g})\ \Gamma_c \vdash n \downarrow n',\ D' = D \cup \{\bar{v}, \bar{n}\},\ D'_i = D_i \cup \{\bar{v}, \bar{n}\}, [\hat{p}] = \bar{v}}{\Gamma_c \triangleright \langle I^\alpha, D\rangle n[\![(c!\langle \hat{p}, \bar{n}\rangle \mid P)]\!]^\ell_r \mid \prod_{i \epsilon I} \langle I^\alpha, D_i\rangle n_i[\![c?(\widetilde{x_i}, \widetilde{y_i})\ P_i]\!]^{\ell_i}_{r_i} \mid M_f \mid M_{\not g} \rightarrow \Gamma_c \triangleright \langle I^\alpha, D'\rangle n[\![P]\!]^{\ell'}_r \mid \prod_{i \epsilon I} \langle I^\alpha, D'_i\rangle n_i[\![P_i\{\bar{v}/\widetilde{x_i}, \bar{n}/\widetilde{y_i}\}]\!]^{\ell'_i}_{r'_i} \mid M'_f \mid M'_{\not g}}$$

(R-*dRi*-IDS)

$$\frac{\alpha \epsilon \{d, f, t\},\ D' = D \cup \{\bar{v}, \bar{n}\},\ d(\ell, \ell') \leq \delta}{\Gamma_c \triangleright \langle I^\alpha, D\rangle n[\![c\ !\langle \hat{v}, \bar{n}\rangle \mid c\ ?(\bar{x}, \bar{y}) P)]\!]^\ell_r \rightarrow \Gamma_c \triangleright \langle I^\alpha, D'\rangle n[\![P\{\bar{v}/\bar{x}, \bar{n}/\bar{y}\}]\!]^{\ell'}_{r'}} \quad [\hat{p}] = \bar{v}$$

(R-*dRi*-e-THEN)

$$\frac{\alpha \epsilon \{e\},\ d(\ell, \ell') \leq \delta}{\Gamma_c \triangleright \langle I^\alpha, D\rangle n[\![if\ b\ then\ P_1\ else P_2]\!]^\ell_r \rightarrow \Gamma_c \triangleright \langle I^\alpha, D'\rangle n[\![P_1]\!]^{\ell'}_{r'}} \quad [b] = true$$

(R-*dRi*-t-THEN)

$$\frac{\alpha \epsilon \{t\},\ d(\ell, \ell') \leq \delta}{\Gamma_c \triangleright \langle I^\alpha, D\rangle n[\![if\ b\ then\ c!\langle 1, \bar{n}\rangle\ else P_2]\!]^\ell_r \rightarrow \Gamma_c \triangleright \langle I^\alpha, D'\rangle n[\![c!\langle 1, \bar{n}\rangle]\!]^{\ell'}_{r'}} \quad [b] = true$$

(R-*dRi*-et-ELSE)

$$\frac{\alpha \epsilon \{e, t\},\ d(\ell, \ell') \leq \delta}{\Gamma_c \triangleright \langle I^\alpha, D\rangle n[\![if\ b\ then\ P_1\ else P_2]\!]^\ell_r \rightarrow \Gamma_c \triangleright \langle I^\alpha, D'\rangle n[\![P_2]\!]^{\ell'}_{r'}} \quad [b] \neq true$$

Fig. 6. Reduction semantics contd

III. Reduction Semantics in *dRi*

Reduction semantics providing dynamics to *dRi*, is defined as a binary relation $\rightarrow$ over networks or processes. Reduction relation $\rightarrow$ for our proposed language *dRi* is specified in Fig. 6 and Fig. 7.

(R-*dRi*-MOVE)

$$\frac{d(\ell,\ell')\leq\delta}{\Gamma_c\rhd\langle I^\alpha,D\rangle n[\![P]\!]^{\ell}_{r}\rightarrow\Gamma_c\rhd\langle I^\alpha,D\rangle n[\![P]\!]^{\ell'}_{r'}}$$

(R-*dRi*-STRUCT)

$$\frac{M_1\equiv M_2,\ \Gamma_c\rhd M_2\rightarrow\Gamma_c\rhd M_2',\ M_2'\equiv M_1'}{\Gamma_c\rhd M_1\rightarrow\Gamma_c\rhd M_1'}$$

(R-*dRi*-CNTX)

$$\frac{\Gamma_c\rhd M\rightarrow\Gamma_c\rhd M'}{\Gamma_c\ M\mid M_1\rightarrow\Gamma_c\rhd M'\mid M_1}$$

$$\frac{\Gamma_c\rhd M\rightarrow\Gamma_c\rhd M'}{\Gamma_c\rhd M_1\mid M\rightarrow\Gamma_c\rhd M_1\mid M'}$$

(R-*dRi*-P-CNTX)

$$\frac{\Gamma_c\rhd\langle I^\alpha,D\rangle n[\![P]\!]^{\ell}_{r}\rightarrow\Gamma_c\rhd\langle I^\alpha,D'\rangle\ n[\![P']\!]^{\ell'}_{r'}}{\Gamma_c\rhd\langle I^\alpha,D\rangle n[\![P|P_1]\!]^{\ell}_{r}\rightarrow\Gamma_c\rhd\langle I^\alpha,D'\rangle n[\![P'|P_1]\!]^{\ell'}_{r'}}$$

Fig. 7. Contd. Reduction semantics

Reduction rule (R-*dRi*-e-COMM) models inter node communication. Node n can send a message $\tilde{v}$ destined to destination node(s) $\tilde{n}$ along external channel c to the node(s) n_i that is(are) within transmission range r of sender node n. Connectivity between two nodes is ensured using network connectivity function Γ_c where $\Gamma_c \bullet\!\!\mapsto n \uparrow n'$. Condition $n \neq n_i$ ensures that here communication can take place between two processes executing at different nodes only. At receiver node n_i, external input process $c?(\tilde{x}_i, \tilde{y}_i)\,P_i$ evolves to $P_i\{\tilde{v}/\tilde{x}_i, \tilde{n}/\tilde{y}_i\}$ assuming that structure of $\tilde{v}$ & $\tilde{x}_i$ and $\tilde{n}$ & $\tilde{y}_i$ exactly match. Data store D and D_i are updated due to the reduction. Since nodes are highly dynamic and need to be energy efficient, they may also change their physical locations from ℓ, ℓ_i to ℓ', ℓ_i' respectively provided $d(\ell,\ell')\leq\delta$ & $d(\ell_i,\ell_i')\leq\delta$ and adjust transmission power from r, r_i to r', r_i' respectively during this computational step of inter node communication. Pre-condition $\neg rec(M_1,c)$ model that $nodes(M_1)$ are not waiting to receive message on common channel c. Pre-condition $\neg rec(M_1,c)$ is negation of $rec(M_1,c)$. Pre-condition $\neg rec(M_1,c)$ models that $nodes(M_1)$ are not waiting to receive message on common channel c. In this reduction rule, no change in system term M_2 after reduction implies that $nodes(M_2)$ are not in transmission range of node n since $\forall n'\varepsilon\, nodes(M_2),\ \Gamma_c \bullet\!\!\mapsto n\downarrow n'$.

The most important is rule (R-*dRi*-IDS) that models conceptual intrusion detection system. It models three components of IDS namely Local data collection d, Feature extraction f and Local detection t as given in Fig. 3. Data store is updated due to internal output IDS process $c!<\hat{v},\tilde{n}>$ and internal input IDS process $c?(\tilde{x},\tilde{y})P$ that evolve to $P\{\tilde{v}/\tilde{x},\tilde{n}/\tilde{y}\}$ at node n where $|\hat{v}|=\tilde{v}$, assuming pattern of $\tilde{v}$ & $\tilde{x}$ and $\tilde{n}$ & $\tilde{y}$ match. During this intra node communication, node n can move from location ℓ to ℓ' such that $d(\ell,\ell')\leq\delta$ where δ is the maximum distance that can be covered by a node in one computational step

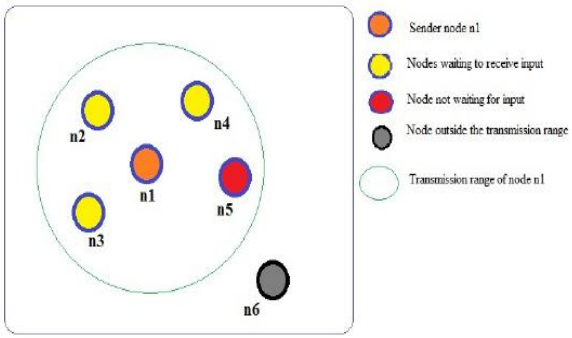

Fig. 8 Example: IDS and mobile ad-hoc networks

Node n may also adjust its transmission range from r to r'. The rule (R-*dRi*-IDS) also models that when intra node reduction takes place, data store D is updated to D'. Rule (R-*dRi*-MOVE) models that node can change its physical location from ℓ to ℓ' and transmission range from r to r' without reducing process P. Rules (R-*dRi*-e-THEN), (R-*dRi*-t-THEN) and (R-*dRi*-et-ELSE) models matching and unmatching construct for system. Rules (R-*dRi*-t-THEN) and (R-*dRi*-et-ELSE) models part of Local Detection component t of IDS. These rules evaluate the expression b with probable form $F \geq thr$ to detect malicious node. True value of detection condition $F \geq thr$ claims that node(s) under consideration $\tilde{n}$ is(are) suspicious. Here F is a value of features extracted from data store e.g., number of packets sent by a node and thr is a predefined threshold value. Reduction rule (R-*dRi*-e-COMM) also models fourth component a of IDS I where it sends alarm message to neighbouring nodes in case of detection of malicious node by local detection model. Rule ((R-*dRi*-STRUCT) states that reduction over network is defined up to structural equivalence. Rule (R-*dRi*-CNTX) preserves

contextuality of reduction relation $\rightarrow$ over network or node whereas rule (R- *dRi* -P-CNTX) preserves contextuality of reduction relation $\rightarrow$ over process. Now we take an example to demonstration detection of an intrusion in *dRi* . An example showing detection of malicious node in MANET is given in next section.

IV. Example

Consider a system configuration $\Gamma_c \triangleright \mathsf{M}$ for a network as shown in Fig. 8, consisting parallel composition of 6 nodes n_1, n_2, ..., n_6. The topology or connectivity of these 6 nodes is shown in Fig. 8. Nodes n_1, n_2, n_3, n_4 and n_5 are within the transmission r of node n_1 at a particular point of time. Thus we have connectivity function as $\Gamma_c \bullet\!\!\mapsto n_1 \uparrow n_2$, $\Gamma_c \bullet\!\!\mapsto n_1 \uparrow n_3$, $\Gamma_c \bullet\!\!\mapsto n_1 \uparrow n_4$, $\Gamma_c \bullet\!\!\mapsto n_1 \uparrow n_5$ and $\Gamma_c \bullet\!\!\mapsto n_1 \downarrow n_6$. Node n_1 acts as a sender node while nodes n_2, n_3 and n_4 as receiver nodes that are waiting to receive input sent by node n_1 on common channel c. Node n_5 is in transmission range of node n_1 that is $\Gamma_c \bullet\!\!\mapsto n_1 \uparrow n_5$ but not waiting to detect value(s) sent by n_1 along channel c.

A typical network M looks like $M_1 \mid M_2 \mid M_3 \mid M_4 \mid M_5 \mid M_6$ where M_1, M_2, M_3, M_4, M_5 and M_6 are sub-system terms corresponding to nodes n_1, n_2, n_3, n_4, n_5 and n_6 respectively. Thus M can be defined as follow:

$$\mathsf{M} = \langle I^{\alpha_1}, D_1\rangle n_1\left[P_1\right]_{r_1}^{\ell_1} \mid \langle I^{\alpha_2}, D_2\rangle n_2\left[P_2\right]_{r_2}^{\ell_2}$$
$$\mid \langle I^{\alpha_3}, D_3\rangle n_3\left[P_3\right]_{r_3}^{\ell_3} \mid \langle I^{\alpha_4}, D_4\rangle n_4\left[P_4\right]_{r_4}^{\ell_4}$$
$$\mid \langle I^{\alpha_5}, D_5\rangle n_5\left[P_5\right]_{r_5}^{\ell_5} \mid \langle I^{\alpha_6}, D_6\rangle n_6\left[P_6\right]_{r_6}^{\ell_6}$$

Here let

$$P_1 \Leftarrow c!\langle \tilde{v}, \tilde{n} \rangle \mid c_f!\langle g(n_1), \tilde{n}_1 \rangle \mid$$
$$c_f?(\tilde{x}_1, \tilde{n}_1)\ \mathit{if}\ h(\tilde{x}_1, thr)\ \mathit{then}\ c_a!\langle 1, \tilde{n}_1 \rangle\ \mathit{else\ stop}$$
$$P_2 \Leftarrow c?(\tilde{x}_2, \tilde{n}_2)P_{21} \mid c_a?(\tilde{x}_2, \tilde{n}_2)P_{22}$$
$$P_3 \Leftarrow c?(\tilde{x}_3, \tilde{n}_3)P_{31} \mid c_a?(\tilde{x}_3, \tilde{n}_3)P_{32}$$
$$P_4 \Leftarrow c?(\tilde{x}_4, \tilde{n}_4)P_{41} \mid c_a?(\tilde{x}_4, \tilde{n}_4)P_{42}$$
$$P_5 \Leftarrow c_a?(\tilde{x}_5, \tilde{n}_5)P_{51}$$
$$P_6 \Leftarrow c_1?(\tilde{x}_6, \tilde{n}_6)P_{61} \mid c_a?(\tilde{x}_6, \tilde{n}_6)P_{62}$$

Here $g(n_1)$ is a feature extraction function that extracts features for node n_1 from data store. Function $h(\tilde{x}_1, thr)$ compares the extracted features $\tilde{x}_1$ to threshold values thr and returns value $true$ or $false$. Since we have $\Gamma_c \mapsto \bullet\ n_1 \uparrow n_2$, $\Gamma_c \bullet\!\!\mapsto n_1 \uparrow n_3$, $\Gamma_c \bullet\!\!\mapsto n_1 \uparrow n_4$, $\Gamma_c \bullet\!\!\mapsto n_1 \uparrow n_5$ and $\Gamma_c \bullet\!\!\mapsto n_1 \downarrow n_6$, using rule R- *dRi* -e-COMM, we can obtain $\Gamma_c \triangleright \mathsf{M} \rightarrow \Gamma_c \triangleright \mathsf{M}'$ where,

$$\mathsf{M}' \equiv \langle I^{\alpha_1}, D_1^1\rangle n_1\left[c_f!\langle g(n_1), \tilde{n}_1 \rangle \mid c_f?(\tilde{x}_1, \tilde{y}_1)\right.$$
$$\left. \mathit{if}\ h(\tilde{x}_1, thr)\ \mathit{then}\ c_a!\langle 1, \tilde{n}'_1 \rangle\ \mathit{else\ stop}\right]_{r_1^1}^{\ell_1^1}$$
$$\mid \langle I^{\alpha_2}, D_2^1\rangle n_2\left[P_{21}\{\tilde{v}/\tilde{x}_2, \tilde{n}/\tilde{y}_2\} \mid c_a?(\tilde{x}_2, \tilde{y}_2)P_{22}\right]_{r_2^1}^{\ell_2^1}$$
$$\mid \langle I^{\alpha_3}, D_3^1\rangle n_3\left[P_{31}\{\tilde{v}/\tilde{x}_3, \tilde{n}/\tilde{y}_3\} \mid c_a?(\tilde{x}_3, \tilde{y}_3)P_{32}\right]_{r_3^1}^{\ell_3^1}$$
$$\mid \langle I^{\alpha_4}, D_4^1\rangle n_4\left[P_{41}\{\tilde{v}/\tilde{x}_4, \tilde{n}/\tilde{y}_4\} \mid c_a?(\tilde{x}_4, \tilde{y}_4)P_{42}\right]_{r_4^1}^{\ell_4^1}$$
$$\mid \langle I^{\alpha_5}, D_5\rangle n_5\left[c_a?(\tilde{x}_5, \tilde{y}_5)P_{51}\right]_{r_5}^{\ell_5}$$
$$\mid \langle I^{\alpha_6}, D_6\rangle n_6\left[c_1?(\tilde{x}_6, \tilde{y}_6)P_{61} \mid c_a?(\tilde{x}_6, \tilde{y}_6)P_{62}\right]_{r_6}^{\ell_6}$$

such that, $\alpha_1 = \alpha_2 = \alpha_3 = \alpha_4 = e$, $D_1^1 = D_1 \cup \{\tilde{v}, \tilde{n}\}$, $D_2^1 = D_2 \cup \{\tilde{v}, \tilde{n}\}$, $D_3^1 = D_3 \cup \{\tilde{v}, \tilde{n}\}$, $D_4^1 = D_4 \cup \{\tilde{v}, \tilde{n}\}$, $d(\ell_1, \ell_1^1) \le \delta$, $d(\ell_2, \ell_2^1) \le \delta$, $d(\ell_3, \ell_3^1) \le \delta$, $d(\ell_4, \ell_4^1) \le \delta$, $d(\ell_5, \ell_5^1) \le \delta$ and, $d(\ell_6, \ell_6^1) \le \delta$.

Based on the statistics collected at the data store of node n_1, it detects node n_2 as a malicious node. After local detection, node n_1 sends alarm message to its neighbouring nodes. Formal description of this system is given below: When $\alpha_1 = f$, using rule R- *dRi* -IDS following reduction takes place

$$\Gamma_c \triangleright \mathsf{M}' \rightarrow \Gamma_c \triangleright \mathsf{M}''$$

where,

$$\mathsf{M}'' \equiv \langle I^{\alpha_1}, D_1^2\rangle n_1\left[\mathit{if}\ h(V_{gn_1}, thr)\ \mathit{then}\ c_a!\langle 1, \tilde{n}_1 \rangle\ \mathit{else}\right.$$
$$\left. \mathit{stop}\right]_{r_1^2}^{\ell_1^2} \mid \langle I^{\alpha_2}, D_2^1\rangle n_2\left[P_{21}\{\tilde{v}/\tilde{x}_2, \tilde{n}/\tilde{y}_2\} \mid c_a?(\tilde{x}_2, \tilde{y}_2)P_{22}\right]_{r_2^1}^{\ell_2^1}$$
$$\mid \langle I^{\alpha_3}, D_3^1\rangle n_3\left[P_{31}\{\tilde{v}/\tilde{x}_3, \tilde{n}/\tilde{y}_3\} \mid c_a?(\tilde{x}_3, \tilde{y}_3)P_{32}\right]_{r_3^1}^{\ell_3^1}$$
$$\mid \langle I^{\alpha_4}, D_4^1\rangle n_4\left[P_{41}\{\tilde{v}/\tilde{x}_4, \tilde{n}/\tilde{y}_4\} \mid c_a?(\tilde{x}_4, \tilde{y}_4)P_{42}\right]_{r_4^1}^{\ell_4^1}$$
$$\mid \langle I^{\alpha_5}, D_5\rangle n_5\left[c_a?(\tilde{x}_5, \tilde{y}_5)P_{51}\right]_{r_5}^{\ell_5}$$
$$\mid \langle I^{\alpha_6}, D_6\rangle n_6\left[c_1?(\tilde{x}_6, \tilde{y}_6)P_{61} \mid c_a?(\tilde{x}_6, \tilde{y}_6)P_{62}\right]_{r_6}^{\ell_6}$$

where, $D_1^2 = D_1^1 \cup \{V_{gn_1}, \tilde{n}_1\}$, $g(n_1) = V_{gn_1}$ and, $d(\ell_1^1, \ell_1^2) \leq \delta$

Immediately after executing f of IDS, next component Local detection t is executed. When $\alpha_1 = t$, using rule R- *dRi* -t-THEN following reduction takes place

$$\Gamma_c \triangleright M'' \rightarrow \Gamma_c \triangleright M'''$$

where, $M''' \equiv \langle I^{\alpha_1}, D_1^3 \rangle n_1[c_a! < 1, n_1 >]_{r_1^3}^{\ell_1^3}$

$$| \langle I^{\alpha_2}, D_2^1 \rangle n_2[P_{21}\{\tilde{v}/\tilde{x}_2, \tilde{n}/\tilde{y}_2\} | c_a?(\tilde{x}_2, \tilde{y}_2)P_{22}]_{r_2^1}^{\ell_2^1}$$

$$| \langle I^{\alpha_3}, D_3^1 \rangle n_3[P_{31}\{\tilde{v}/\tilde{x}_3, \tilde{n}/\tilde{y}_3\} | c_a?(\tilde{x}_3, \tilde{y}_3)P_{32}]_{r_3^1}^{\ell_3^1}$$

$$| \langle I^{\alpha_4}, D_4^1 \rangle n_4[P_{41}\{\tilde{v}/\tilde{x}_4, \tilde{n}/\tilde{y}_4\} | c_a?(\tilde{x}_4, \tilde{y}_4)P_{42}]_{r_4^1}^{\ell_4^1}$$

$$| \langle I^{\alpha_5}, D_5 \rangle n_5[c_a?(\tilde{x}_5, \tilde{y}_5)P_{51}]_{r_5}^{\ell_5}$$

$$| \langle I^{\alpha_6}, D_6 \rangle n_6[c_1?(\tilde{x}_6, \tilde{y}_6)P_{61} | c_a?(\tilde{x}_6, \tilde{y}_6)P_{62}]_{r_6}^{\ell_6}$$

where, $D_1^3 = D_1^2 \cup \{V_{gn_1}, n_1\}$, $h(V_{gn_1}, thr) = true$ and, $d(\ell_1^2, \ell_1^3) \leq \delta$.

Suppose $\Gamma_c \bullet\!\!\mapsto n_1 \uparrow n_2$, $\Gamma_c \bullet\!\!\mapsto n_1 \uparrow n_3$, $\Gamma_c \bullet\!\!\mapsto n_1 \uparrow n_4$, $\Gamma_c \bullet\!\!\mapsto n_1 \uparrow n_5$ and $\Gamma_c \bullet\!\!\mapsto n_1 \downarrow n_6$, using rule R- *dRi* -e-COMM, we can obtain $\Gamma_c \triangleright M'''$

$$\rightarrow \Gamma_c \triangleright \langle I^{\alpha_1}, D_1^4 \rangle n_1[stop]_{r_1^4}^{\ell_1^4}$$

$$| \langle I^{\alpha_2}, D_2^2 \rangle n_2[P_{21}\{\tilde{v}/\tilde{x}_2, \tilde{n}/\tilde{y}_2\} | P_{22}\{1/\tilde{x}_2, n_1/\tilde{y}_2\}]_{r_2^2}^{\ell_2^2}$$

$$| \langle I^{\alpha_3}, D_3^2 \rangle n_3[P_{31}\{\tilde{v}/\tilde{x}_3, \tilde{n}/\tilde{y}_3\} | P_{32}\{1/\tilde{x}_3, n_1/\tilde{y}_3\}]_{r_3^2}^{\ell_3^2}$$

$$| \langle I^{\alpha_4}, D_4^2 \rangle n_4[P_{41}\{\tilde{v}/\tilde{x}_4, \tilde{n}/\tilde{y}_4\} | P_{42}\{1/\tilde{x}_4, n_1/\tilde{y}_4\}]_{r_4^1}^{\ell_4^1}$$

$$| \langle I^{\alpha_5}, D_5^2 \rangle n_5[P_{51}\{1/\tilde{x}_5, n_1/\tilde{y}_5\}]_{r_5^1}^{\ell_5^1}$$

$$| \langle I^{\alpha_6}, D_6 \rangle n_6[c_1?(\tilde{x}_6, \tilde{y}_6)P_{61} | c_a?(\tilde{x}_6, \tilde{y}_6)P_{62}]_{r_6}^{\ell_6}$$

where, $D_1^4 = D_1^3 \cup \{1, n_1\}$, $D_2^2 = D_2^1 \cup \{1, n_1\}$, $D_3^2 = D_3^1 \cup \{1, n_1\}$, $D_4^2 = D_4^1 \cup \{1, n_1\}$, $D_5^2 = D_5^1 \cup \{1, n_1\}$, $d(\ell_1^3, \ell_1^4) \leq \delta$, $d(\ell_2^1, \ell_2^2) \leq \delta$, $d(\ell_3^1, \ell_3^2) \leq \delta$, $d(\ell_4^1, \ell_4^2) \leq \delta$ and $d(\ell_5, \ell_5^1) \leq \delta$. Nodes B and C may further broadcast the alarm message to its neighbouring nodes and so on. Equivalency of *dRi* (implementation) with E-BUM [19] (specification) is given in next section.

V. Equivalency of *dRi* with E-BUM [19]

The reduction equivalency of our proposed formal language *dRi* is supported by its equivalency established with already verified formal language [19] designed to model basic properties of mobile ad hoc networks.

A. Key Features and Limitations of E-BUM [19]

A typical node in E-BUM [19] looks $n[P]_l$. Each node is assigned with network address n, physical location ℓ and executing process P [2]. In E-BUM [19], distance function is used to ensures connectivity among nodes. Distance function, defined as $d(.,.)$, takes locations of the two nodes as input and returns their distance as output. [19] supports rules for broadcast, unicast and multicast communication. It allows node to model the ability of a node to adjust its transmission range and move in and out of the transmission range of other nodes in the networks.

This calculus does not support concept of store to record routing table, node failure and security. This calculus [19] has not been modelled to support any detection and response system in MANETs. Our proposed formal language models detection & response system that is intrusion detection system to detect external or internal malicious node in MANETs.

To establish reduction equivalency between our proposed language *dRi*, designed to model IDS in MANETs, and E-BUM, designed to model basic properties of MANETs, a Filter $\mathfrak{I}$ is defined and a theorem supporting this equivalency is proved. Definition of Filter function $\mathfrak{I}$ is explained below:

(F-MM)	$\mathfrak{I}(M_1 \mid M_2)$	=	$\mathfrak{I}(M_1) \mid \mathfrak{I}(M_2)$
(F-ϵ)	$\mathfrak{I}(\epsilon)$	=	0
(F-IP)	$\mathfrak{I}(\langle I^{\alpha}, D \rangle\, n[\![P]\!]_r^{\ell})$	=	$n[\![P]\!]^{\ell}$
(F-IStop)	$\mathfrak{I}(\langle I^{\alpha}, D \rangle\, n[\![stop]\!]_r^{\ell})$	=	$n[\![stop]\!]^{\ell}$
(F-I!)	$\mathfrak{I}(\langle I^{\alpha}, D \rangle\, n[\![c! < \tilde{v}, \tilde{n} >]\!]_r^{\ell})$	=	$n[\![c! < \tilde{v}, \tilde{n}]\!]_r^{\ell}$
(F-I?)	$\mathfrak{I}(\langle I^{\alpha}, D \rangle\, n[\![c?(\tilde{x}, \tilde{y})P]\!]_r^{\ell})$	=	$n[\![c?(\tilde{x}, \tilde{y})P]\!]^{\ell}$
(F-Iif)	$\mathfrak{I}(\langle I^{\alpha}, D \rangle\, n[\![if\ b\ then\ P_1\ else\ P_2]\!]_r^{\ell})$	=	$n[\![if\ b\ then\ P_1\ else\ P_2]\!]^{\ell}$
(F-IPar)	$\mathfrak{I}(\langle I^{\alpha}, D \rangle\, n[\![P_1 \mid P_2]\!]_r^{\ell})$	=	$n[\![stop]\!]^{\ell}$
(F-IRec)	$\mathfrak{I}(\langle I^{\alpha}, D \rangle\, n[\![*P]\!]_r^{\ell})$	=	$n[\![*P]\!]^{\ell}$

Fig. 9. Filter function

B. Definition of Filter Function $\mathfrak{I}$:

Formal definition of Filter function $\mathfrak{I}$ can be defined as follow:

$$\mathfrak{I} : \mathsf{M}_{dRi} \rightarrow M_{E-BUM}$$

Filter function $\mathfrak{I}$ shows mapping from system terms defined in M_{dRi} to system terms defined in M_{E-BUM}.

$\mathfrak{I}$ is applied on the syntax defined in M_{dRi} and produces syntax defined in M_{E-BUM}. $\mathfrak{I}$ can filter out details of the IDS from the syntax for M_{dRi} and can produce each of the respective form of syntax defined in M_{E-BUM}. Capability of $\mathfrak{I}$ is expressed in rules given in Fig. 9. Before we prove theorems about the reduction equivalence of dRi and E-BUM [19] systems, we will see the following propositions about some properties of the function =.

Proposition 1 *For any system term S in dRi such that $\mathfrak{I}(S) = R$ and $R \equiv R'$ implies that there exists some system term S' in dRi such that $\mathfrak{I}(S') = R'$ and $S \equiv S'$.*

Proof This can be proved by induction on various forms of S.

Case 1: Suppose S is of form ε. This case is trivial.

Case 2: Consider S is of form $\langle I^{\alpha}, D\rangle n[P]_r^{\ell}$. Since we know that $\mathfrak{I}(S) = R$, using F-IP rule given in figure 3, we can obtain that:

$$\mathfrak{I}(\langle I^{\alpha}, D\rangle n[P]_r^{\ell}) = n[P]^{\ell}$$

Since $R \equiv R'$, thus using rule (Struct Zero Par), R' should be of form $n[P]^{\ell} \mid 0$. Suppose there is some S' that is of form $\langle I^{\alpha}, D\rangle n[P]_r^{\ell} \mid \varepsilon$. Using rule (M-STOP) we can obtain that

$$\langle I^{\alpha}, D\rangle n[P]_r^{\ell} \equiv \langle I^{\alpha}, D\rangle n[P]_r^{\ell} \mid \varepsilon$$

Now we need to prove that $\mathfrak{I}(S') = R'$. We have assumed that S' is of form $\langle I^{\alpha}, D\rangle n[P]_r^{\ell} \mid \varepsilon$. Using rule (F-MM) we can obtain

$$\mathfrak{I}(\langle I^{\alpha}, D\rangle n[P]_r^{\ell} \mid \varepsilon) = \mathfrak{I}(\langle I^{\alpha}, D\rangle n[P]_r^{\ell}) \mid \mathfrak{I}(\varepsilon)$$

Since using rule (F-IP) and (F-ε) we know that

$$\mathfrak{I}(\langle I^{\alpha}, D\rangle n[P]_r^{\ell}) = n[P]^{\ell}$$

and

$$\mathfrak{I}(\varepsilon) = 0$$

Thus we can obtain

$$\mathfrak{I}(\langle I^{\alpha}, D\rangle n[P]_r^{\ell} \mid \varepsilon) = R'$$

where, R' is of form $n[P]^{\ell} \mid 0$.

Case 3: Consider S is of form $S_1 \mid S_2$. Using F-MM rule given in figure 3, we can obtain that :

$$\mathfrak{I}(S_1 \mid S_2) = \mathfrak{I}(S_1) \mid \mathfrak{I}(S_2)$$

where, $\mathfrak{I}(S_1) = R_1$, $\mathfrak{I}(S_2) = R_2$.

Thus we can obtain

$$\mathfrak{I}(S_1 \mid S_2) = \mathfrak{I}(S_1) \mid \mathfrak{I}(S_2) = R_1 \mid R_2$$

We know that $\mathfrak{I}(S) = R$ where, R is of form $R_1 \mid R_2$. Since $R \equiv R'$, thus using rule (Struct Par Comm), R' should be of form $R_2 \mid R_1$. Suppose there is some S' that is of form $S_2 \mid S_1$. Using rule (M-COM) we can obtain that

$$S_1 \mid S_2 \equiv S_2 \mid S_1$$

Now we need to prove that $\mathfrak{I}(S') = R'$. We have assumed that S' is of form $S_2 \mid S_1$. Using rule (F-MM) we can obtain

$$\mathfrak{I}(S_2 \mid S_1) = \mathfrak{I}(S_2) \mid \mathfrak{I}(S_1)$$

We know that $\mathfrak{I}(S_2) = R_2$ and $\mathfrak{I}(S_1) = R_1$,

Thus we can obtain

$$\mathfrak{I}(S_2 \mid S_1) = \mathfrak{I}(S_2) \mid \mathfrak{I}(S_1) = R'$$

where, R' is of form $R_2 \mid R_1$.

Case 4: Consider S is of form $\langle I^{\alpha}, D\rangle n[P \mid P_1]_r^{\ell}$. Since we know that $\mathfrak{I}(S) = R$, using rule F-IPar we can obtain

$$\mathfrak{I}(\langle I^{\alpha}, D\rangle n[P \mid P_1]_r^{\ell}) = n[stop]^{\ell}$$

where, $n[stop]^{\ell}$ is a system term in E-BUM. Using rule Struct Stop, we know that

$$n[stop]^{\ell} \equiv 0$$

Now using rules (P-COM) and (M-EQ), we can obtain

$$\langle I^{\alpha}, D\rangle n[P \mid P_1]_r^{\ell} = \langle I^{\alpha}, D\rangle n[P_1 \mid P]_r^{\ell}$$

Again using rule F-IPar, we can obtain

$$\mathfrak{I}(\langle I^{\alpha}, D\rangle n[P_1 \mid P]_r^{\ell}) = n[stop]^{\ell}$$

Case 4: One of possible forms S is $\langle I^{\alpha}, D\rangle n[if\ b\ then\ c! < 1, \tilde{n} > else\ P_2]_r^{\ell}$. Since we know that $\mathfrak{I}(S) = R$, using rule F-Iif we can obtain

$$\mathfrak{I}(\langle I^{\alpha}, D\rangle n[if\ b\ then\ c! < 1, \tilde{n} > else\ P_2]_r^{\ell}) = n[if\ b\ then\ P_1\ else\ P_2]^{\ell}$$

where, $n[if\ b\ then\ P_1\ else\ P_2]^{\ell}$ is a system term in E-BUM. Using rules Struct Then, R-CIDSM-t-THEN and R- CIDSM-STRUCT given in Fig. 3 this case can be proved. Similarly when S is of form $\langle I^{\alpha}, D\rangle n[if\ b\ then\ P_1\ else\ P_2]_r^{\ell}$, Struct Then & R-CIDSM-e-THEN when $b = true$ or Struct Else, R-CIDSM-et-ELSE when $b \neq true$ and R-CIDSM-STRUCT can be applied to proof the case.

Proposition 2 For any system term S in *dRi* $S \equiv S'$ implies $\Im(S) \equiv \Im(S')$.

Proof This can be proved by induction on the definition of $\equiv$ for CIDSM. Suppose S is of form $S_1 \mid S_2$. Using rule M-COM we can obtain

$$S_1 \mid S_2 = S_2 \mid S_1$$

Thus S' should be of form $S_2 \mid S_1$. Using F-MM rule given in Fig. 8, we can obtain that:

$$\Im(S_1 \mid S_2) = \Im(S_1) \mid \Im(S_2)$$

where, $\Im(S_1) = R_1$, $\Im(S_2) = R_2$

Thus we can obtain

$$\Im(S_1 \mid S_2) = \Im(S_1) \mid \Im(S_2) = R_1 \mid R_2$$

We know that $\Im(S) = R$ where, R is of form $R_1 \mid R_2$. Similarly, we can obtain that

$$\Im(S_2 \mid S_1) = \Im(S_2) \mid \Im(S_1) = R_2 \mid R_1$$

Using rule (Struct Par Comm),we know that

$$R_1 \mid R_2 \equiv R_2 \mid R_1$$

Thus we can obtain

$$\Im(S_1 \mid S_2) \equiv \Im(S_2 \mid S_1)$$

Similarly other cases for the forms of S defined over $\equiv$ relation can be proved.

Lemma 1 In *dRi*, if a well formed configuration $\Gamma_c \rhd S$ does a reduction $\Gamma_c \rhd S \xrightarrow{*} \Gamma_c \rhd S'$ and $\Im(S) = R$, where R is a system term in E-BUM, then

• either there exists a system term R' in E-BUM such that $R \rightarrow R'$ and $\Im(S') = R'$.

• or $\Im(S') = R$

Proof This can be proved using rule induction on the derivation of $\Gamma_c \rhd S \xrightarrow{*} \Gamma_c \rhd S'$ where $\Im(S) = R$. We take all cases as follows:

Case 1: Suppose S is of form ε. This case is trivial.

Case 2: Consider S is of form $\langle I^\alpha, D\rangle n[P]^\ell_r$. Using R-CIDSM-MOVE rule given in Fig. 6, $\Gamma_c \rhd \langle I^\alpha, D\rangle n[P]^\ell_r$ can be reduced as follow:

$$\Gamma_c \rhd \langle I^\alpha, D\rangle n[P]^\ell_r \rightarrow \Gamma_c \rhd \langle I^\alpha, D\rangle n[P]^{\ell'}_{r'}$$

where, $d(\ell, \ell') \le \delta$

Since $\Im(S) = R$, thus R should be of form nP^ℓ.

Using R-Move rule defined in E-BUM, $n[P]^\ell$ can be reduced as follow:

$$n[P]^\ell \rightarrow n[P]^{\ell'} \text{ where, } d(\ell, \ell') \le \delta$$

$$\Im(\Gamma_c \rhd \langle I^\alpha, D\rangle n[P]^{\ell'}_{r'}) = n[P]^{\ell'}$$

Case 3: Consider S is of form $S_1 \mid S_2$. Using R-CIDSM-CNTX rule given in figure 6, $S_1 \mid S_2$ can be reduced as follow:

$$\Gamma_c \rhd S_1 \mid S_2 \rightarrow \Gamma_c \rhd S_1 \mid S_2'$$

where, $\Gamma_c \rhd S_2 \rightarrow \Gamma_c \rhd S_2'$ Since $\Im(S) = R$, thus R should be of form $R_1 \mid R_2$. Using Struct Par Comm defined in E-BUM, we can obtain

$$R_1 \mid R_2 \equiv R_2 \mid R_1$$

Applying R-Par rule defined in E-BUM, $R_2 \mid R_1$ can be reduced as follow:

$$R_2 \mid R_1 \rightarrow R_2' \mid R_1$$

Again using Struct Par Comm defined in E-BUM, we can obtain

$$R_2' \mid R_1 \equiv R_1 \mid R_2'$$

where, $\Im(S_1 \mid S_2') = R_1 \mid R_2'$

Other possible case when S is of form $S_1 \mid S_2$ and $\Gamma_c \rhd S \rightarrow \Gamma_c \rhd S'$ because $\Gamma_c \rhd S_1 \rightarrow \Gamma_c \rhd S_1'$ can be proved similarly.

Case 4: Consider S is of form $\langle I^\alpha, D\rangle n[c!<\tilde{v}, \tilde{n}>\mid P]^\ell_r \mid \prod_{i\varepsilon I}\langle I^\alpha, D\rangle n_i[c?(\tilde{x}_i, \tilde{n}_i)\ P_i]^{\ell_i}_{r_i} \mid S_1 \mid S_2$.

Using R-CIDSM-e-COMM rule given in Fig. 6, $\langle I^\alpha, D\rangle n[c!<\tilde{v}, \tilde{n}>\mid P]^\ell_r \mid \prod_{i\varepsilon I}\langle I^\alpha, D\rangle n_i[c?(\tilde{x}_i, \tilde{n}_i)\ P]^{\ell_i}_{r_i} \mid S_1 \mid S_2$ Can be reduced as follow: $\Gamma_c \rhd \langle I^\alpha, D\rangle n[c!<\tilde{v}, \tilde{n}>\mid P]^\ell_r \mid \prod_{i\varepsilon I}\langle I^\alpha, D\rangle n_i[c?(\tilde{x}_i, \tilde{n}_i)\ P_i]^{\ell_i}_{r_i} \mid S_1 \mid S_2 \rightarrow \Gamma_c \rhd \langle I^\alpha, D'\rangle n[P]^{\ell'}_{r'} \mid \prod_{i\varepsilon I}\langle I^\alpha, D'\rangle n_i[P_i\{\tilde{v}/\tilde{x}_i, \tilde{n}/\tilde{n}_i\}]^{\ell'_i}_{r'_i} \mid S_1 \mid S_2$

where,

$\forall i \varepsilon N, \Gamma_c \bullet\!\!\mapsto n \uparrow n_i, d(\ell, \ell') \le \delta, d(\ell_i, \ell'_i) \le \delta, n \ne n_i,$

$\alpha \varepsilon \{e\}, \neg rec(S_1, c)\ \forall n' \varepsilon\ nodes(S_2)\ \Gamma_c \bullet\!\!\mapsto n \downarrow n',$

$D' = D \cup \{\tilde{v}, \tilde{n}\}, D'_i = D_i \cup \{\tilde{v}, \tilde{n}\}$

Since $\Im(S) = R$, thus R should be of form as follow:

$n[c!<\tilde{v}, \tilde{n}>\mid P]^\ell \mid \prod_{i\varepsilon I}\langle I^\alpha, D\rangle n_i[c?(\tilde{x}_i, \tilde{n}_i)\ P]^{\ell_i}_{r_i} \mid R_1 \mid R_2$

Applying R-Bcast and R-Par rule defined in E-BUM $n[c!<\tilde{v}, \tilde{n}>\mid P]^\ell \mid \prod_{i\varepsilon I} n_i[c?(\tilde{x}_i, \tilde{n}_i)\ P_i]^{\ell_i} \mid R_1 \mid R_2$ can be reduced as follow:

$n[c!<\tilde{v},\tilde{n}>|P]^{\ell} \mid \prod_{i\in I} n_i[c?(\tilde{x}_i,\tilde{n}_i)\ P_i]^{\ell_i} \mid R_1 \mid R_2$
$\rightarrow n[P]^{\ell'} \mid \prod_{i\in I} n_i[P_i\{\tilde{v}/\tilde{x}_i,\tilde{n}/\tilde{n}_i\}]^{\ell'_i} \mid R_1 \mid R_2$

where, $\forall$ i ε I, $d(\ell,\ell') \le \delta$, $d(\ell_i,\ell'_i) \le \delta$ such that,

$\Im(\langle I^{\alpha},D'\rangle n[P]^{\ell'}_{r'} \mid \prod_{i\in I}\langle I^{\alpha},D'\rangle n_i[P_i\{\tilde{v}/\tilde{x}_i,n/\tilde{n}_i\}]^{\ell'_i}_{r'_i}$
$\mid S_1 \mid S_2) = n[P]^{\ell'} \mid \prod_{i\in I} n_i[P_i\{\tilde{v}/\tilde{x}_i,n/\tilde{n}_i\}]^{\ell'_i} \mid R_1 \mid R_2$

Case 4: Consider S is of form $\langle I^{\alpha},D\rangle n\,[c!<\tilde{v},\tilde{n}>|\,c?(\tilde{x},\tilde{y})P]^{\ell}_r$. Using R-CIDSM-IDS rule given in figure 6, $\langle I^{\alpha},D\rangle n\,c!<\tilde{v},\tilde{n}>|\,c?(\tilde{x},\tilde{y})P^{\ell}_r$ can be reduced as follow:

$$\Gamma_c \rhd \langle I^{\alpha},D\rangle n\,[c!<\tilde{v},\tilde{n}>|\,c?(\tilde{x},\tilde{y})P]^{\ell}_r \rightarrow \Gamma_c \rhd \langle I^{\alpha},D'\rangle n[P\{\tilde{v}/\tilde{x},n/\tilde{y}\}]^{\ell'}_{r'}$$

where, $\alpha\varepsilon\{d,\ f,\ t\}, D' = D\cup\{\tilde{v},\tilde{n}\}$ and $d(\ell,\ell') \le \delta$ Since $\Im(S) = R$, thus R should be of form $\mathrm{n}[\mathrm{P}]^{\ell}$. Applying Struct Then, Sturct Else and Sturct Rec rules defined in E-BUM, $\mathrm{n}[\mathrm{P}]^{\ell}$ can be reduced as follow:

$$\mathrm{n}[\mathrm{P}]^{\ell} \rightarrow \mathrm{n}[\mathrm{P}']^{\ell'}$$

where, $\mathrm{P} \rightarrow \mathrm{P}'$ and $\mathrm{d}(\ell,\ell') \le \delta$ such that,

$$\Im(\langle I^{\alpha},D'\rangle n[P\{\tilde{v}/\tilde{x},n/\tilde{y}\}]^{\ell'}_{r'}) \cong \mathrm{n}[\mathrm{P}']^{\ell'}$$

Case 5: Consider S is of form $\langle I^{\alpha},D\rangle n[P \mid P_1]^{\ell}_r$. Using R-CIDSM-P-CNTX rule given in figure 6, $\langle I^{\alpha},D\rangle n[P \mid P_1]^{\ell}_r$ can be reduced as follow:

$$\langle I^{\alpha},D\rangle n[P \mid P_1]^{\ell}_r \rightarrow \langle I^{\alpha},D'\rangle n[P' \mid P_1]^{\ell'}_{r'}$$

where, $\langle I^{\alpha},D\rangle n[P]^{\ell}_r \rightarrow \langle I^{\alpha},D'\rangle n[P']^{\ell'}_{r'}$ Since $\Im(S) = R$, thus R should be of form $n[\ P \mid Q\ ]^{\ell}$ where, $Q \equiv 0$. Applying Struct Then, Sturct Else or Sturct Rec rules defined in E-BUM, $\mathrm{n}[\ \mathrm{P} \mid \mathrm{Q}\ ]^{\ell}$ can be reduced as follow:

$$\mathrm{n}[\ \mathrm{P} \mid \mathrm{Q}\ ]^{\ell} \rightarrow \mathrm{n}[\ \mathrm{P}' \mid \mathrm{Q}\ ]^{\ell}$$

where, $\mathrm{P} \rightarrow \mathrm{P}'$ such that,

$$\Im(\langle I^{\alpha},D'\rangle n[P' \mid P_1]^{\ell'}_{r'}) \cong \mathrm{n}[\ \mathrm{P}' \mid \mathrm{Q}\ ]^{\ell}$$

Similarly other cases when forms of S are like $\langle I^{\alpha},D\rangle n[\mathit{if}\ b\ \mathit{then}\ P_1\ \mathit{else}\ P_2]^{\ell}_r$ and $\langle I^{\alpha},D\rangle n[\mathit{if}\ b\ \mathit{then}\ c!<1,\tilde{n}>\ \mathit{else}\ P_2]^{\ell}_r$ using rule R-CIDSM-e-THEN, R-CIDSM-ELSE or R-CIDSM-t-THEN rule given in Fig. 6, can be proved.

Lemma 2 If a E-BUM system R does a reduction $R \rightarrow R'$ and $\Im(S) = R_1$ such that $R \equiv R_1$ where S is a system term over a well formed configuration $\Gamma_c \rhd S$ in dRi, then $\Gamma_c \rhd S \xrightarrow{*} \Gamma_c \rhd S'$ such that $\Im(S') = R_2$ and $R' \equiv R_2$.

Proof This can be proved using rule induction on the inference of a E-BUM system reduction $R \rightarrow R'$ and syntactic analysis of S such that $\Im(S) = R_1$ where $R \equiv R_1$. We take all cases as follows:

Case 1: Suppose R is of form 0. This case is trivial.

Case 2: Consider R is of form $\mathrm{n}[\mathrm{P}]^{\ell}$. Using R-Move rule defined in E-BUM, $\mathrm{n}[\mathrm{P}]^{\ell}$ can be reduced as follow:

$$\mathrm{n}[\mathrm{P}]^{\ell} \rightarrow \mathrm{n}[\mathrm{P}]^{\ell'}$$

where, $\mathrm{d}(\ell,\ell') \le \delta$ and $R' \equiv n[P]^{\ell'}$

A system term S in dRi, such that $\Im(S) = R_1$ where $R \equiv R_1$, can take various forms. We shall examine each of them as follow:

Case 2a: We take the case where S is structurally equivalent to $\langle I^{\alpha},D\rangle n[P]^{\ell}_r$ for some α, D and r. Using rule F-IP, we can clearly see that

$$\Im(S) = n[P]^{\ell}$$

where, $n[P]^{\ell} \equiv R$. We know that $\Gamma_c \rhd S$ is a well formed system and therefore $\Gamma_c \rhd S$ does the following reduction using rule R-CIDSM-MOVE given in Fig. 6:

$$\Gamma_c \rhd \langle I^{\alpha},D\rangle n[P]^{\ell}_r \rightarrow \Gamma_c \rhd \langle I^{\alpha},D\rangle n[P]^{\ell'}_{r'}$$

where, $d(\ell,\ell') \le \delta$ and $S' \equiv \Gamma_c \rhd \langle I^{\alpha},D\rangle n[P]^{\ell'}_{r'}$ Using rule F-IP, we can obtain $\Im(S') = n[P]^{\ell'}$ where, $n[P]^{\ell'} \equiv R'$.

Case 2b: We take the case where S is structurally equivalent to $\langle I^{\alpha},D\rangle n[P]^{\ell}_r \mid \varepsilon$ for some α, D and r. Using rule F-IP, we can clearly see that

$$\Im(S) = \Im(\langle I^{\alpha},D\rangle n[P]^{\ell}_r) \mid \Im(\varepsilon)$$

where, $\Im(\langle I^{\alpha},D\rangle n[P]^{\ell}_r = R_{11}$, $\Im(\varepsilon) = R_{12}$ and $R_1 \equiv R_{11} \mid R_{12}$. Using rule Struct-Zero-Par, we can easily obtain

$$R \equiv R_{11} \mid R_{12}$$

We know that $\Gamma_c \rhd S$ is a well formed system and therefore $\Gamma_c \rhd S$ does the following reduction using rule R-CIDSM-MOVE given in Fig. 3.

$$\Gamma_c \rhd \langle I^\alpha, D\rangle n[P]_r^\ell \rightarrow \Gamma_c \rhd \langle I^\alpha, D\rangle n[P]_{r'}^{\ell'}$$

where, $d(\ell, \ell') \leq \delta$ and $S' \equiv \Gamma_c \rhd \langle I^\alpha, D\rangle n[P]_{r'}^{\ell'}$ Using rule F-IP, we can obtain $\Im(S') = n[P]^{\ell'}$ where, $n[P]^{\ell'} \equiv R'$.

Case 3: Now we consider the case of compositional reduction of a E-BUM systems. Let us assume that a E-BUM system term R is of form $R_{11} \mid R_{12}$. Using Struct Par Comm defined in E-BUM, we can obtain

$$R_{11} \mid R_{12} \equiv R_{12} \mid R_{11}$$

Using R-Par rule defined in E-BUM, $R_{12} \mid R_{11}$ can be reduced as follow:

$$R_{12} \mid R_{11} \rightarrow R'_{12} \mid R_{11}$$

because $R_{12} \rightarrow R'_{12}$ Again using Struct Par Comm defined in E-BUM, we can obtain

$$R'_{12} \mid R_{11} \equiv R_{11} \mid R'_{12}$$

Let us assume that a system term S, in CIDSM is of form $S_{11} \mid S_{12}$ such that $\Im(S_{11}) = R_{111}$ and $\Im(S_{12}) = R_{112}$. We know that $\Gamma_c \rhd S$ is a well formed system and therefore $\Gamma_c \rhd S$ does the following reduction using rule R-CIDSM-CNTX given in Fig. 6:

$$\Gamma_c \rhd S \rightarrow \Gamma_c \rhd S'$$

such that $\Im(S') = R_2$ where, $\Gamma_c \rhd S_{12} \rightarrow \Gamma_c \rhd S'_{12}$ and $S' \equiv S_{11} \mid S'_{12}$. We also know that $\Im(S_{11} \mid S'_{12}) = \Im(S_{11}) \mid \Im(S'_{12})$. Since $\Im(S_{11}) = R_{111}$, $\Im(S'_{12}) = R_{212}$, therefore $\Im(S'_{11} \mid S_{12}) = R_{111} \mid R_{212}$. Further we already know that $\Im(S') = R_2$. Now it is obvious to show that $R_2 \equiv R_{111} \mid R_{212}$ and $R' \equiv R_2$.

Similarly the case when a E-BUM system term R is of form $R_{11} \mid R_{12}$ and $R \rightarrow R'$ because $R_{11} \rightarrow R'_{11}$ can be proved using R-Par rule defined in E-BUM and rule R-CIDSM-CNTX given in Fig. 6. **Case 4:** Consider R is of form $n[c!<\tilde{v}, \tilde{n}>|P]^\ell \mid \prod_{i\varepsilon I}\langle I^\alpha, D\rangle n_i[c?(\tilde{x}_i, \tilde{n}_i)\ P_i]^{\ell_i} \mid M_1 \mid M_2$.

Using R-Bcast and R-Par rules defined in E-BUM, R can be reduced to R' where,

$$R' \equiv n[P]^{\ell'} \mid \prod_{i\varepsilon I} n_i[P_i\{\tilde{v}/\tilde{x}_i, \tilde{n}/\tilde{n}_i\}]^{\ell'_i} \mid M_1 \mid M_2$$

Such that, $\forall\ i\ \varepsilon\ I, d(\ell, \ell') \leq \delta, d(\ell_i, \ell'_i) \leq \delta$.

Let us assume that S is of form $\langle I^\alpha, D\rangle n[c!<\tilde{v}, \tilde{n}>|P]_r^\ell \mid \prod_{i\varepsilon I}\langle I^\alpha, D\rangle n_i[c?(\tilde{x}_i, \tilde{n}_i)\ P_i]_{r_i}^{\ell_i} \mid M_1 \mid M_2$, such that $\Im(S) = R_1$. where, $R_1 \equiv n[P]^{\ell'} \mid \prod_{i\varepsilon I} n_i[P_i\{\tilde{v}/\tilde{x}_i, \tilde{n}/\tilde{n}_i\}]^{\ell'_i} \mid M_1 \mid M_2$.

Using R-CIDSM-COMM rule given in Fig. 6, S can be reduced as follow:

$$\Gamma_c \rhd S \rightarrow \Gamma_c \rhd S'$$

where,

$\forall i \varepsilon N, \Gamma_c \bullet\!\!\mapsto n \uparrow n_i, d(\ell, \ell') \leq \delta, d(\ell_i, \ell'_i) \leq \delta, n \neq n_i,$
$\alpha\varepsilon\{e\}, \neg rec(M_1, c)\ \forall n' \varepsilon\ nodes(M_2)\ \Gamma_c \bullet\!\!\mapsto n \downarrow n',$
$D' = D \cup \{\tilde{v}, \tilde{n}\}, D'_i = D_i \cup \{\tilde{v}, \tilde{n}\}$
such that,
$S' \equiv \langle I^\alpha, D'\rangle n[P]_{r'}^{\ell'} \mid \prod_{i\varepsilon I}\langle I^\alpha, D'\rangle n_i[P_i\{\tilde{v}/\tilde{x}_i, \tilde{n}/\tilde{n}_i\}]_{r'_i}^{\ell'_i}$
$\mid M_1 \mid M_2$
$\Im(\langle I^\alpha, D'\rangle n[P]_{r'}^{\ell'} \mid \prod_{i\varepsilon I}\langle I^\alpha, D'\rangle n_i[P_i\{\tilde{v}/\tilde{x}_i, \tilde{n}/\tilde{n}_i\}]_{r'_i}^{\ell'_i}$
$\mid M_1 \mid M_2) \equiv R_2$
where

$$R_1 \equiv n[P]^{\ell'} \mid \prod_{i\varepsilon I} n_i[P_i\{\tilde{v}/\tilde{x}_i, \tilde{n}/\tilde{n}_i\}]^{\ell'_i} \mid M_1 \mid M_2$$

and

$$R' \equiv R_2$$

Similarly the other two cases when a E-BUM system term R is of form $n[if\ b\ then\ P_1\ else\ P_2]^\ell$ using Struct Then rule defined in E-BUM can be proved.

Theorem 1 If $\Im(S) = R$ and $\Gamma_c \rhd S \xrightarrow{*} \Gamma_c \rhd S'$ iff $R \rightarrow R'$ such that $\Im(S') = R'$.

Proof: From Lemma 1 and Lemma 2 this proof is straight-forward.

In Lemma 1, we proved that whenever a well formed configuration in *dRi* does a reduction there exist a corresponding E-BUM [19] system which either does nothing or does a reduction where residuals of both *dRi* and E-BUM [19] systems are matched up to structural equivalence. Similarly for the converse, in Lemma 2 we proved that whenever a E-BUM [19] system does a reduction there exists a corresponding well formed configuration in *dRi* which can do a number of reductions such that the residual are equivalent up to structural equivalence after = abstraction of the residual system in *dRi*. In Theorem 1, systems in both E-BUM [19] and *dRi*. are proven to match up to structural equivalence under reduction semantics. The reduction equivalency between *dRi* and E-BUM [19] designed to model basic properties of mobile ad hoc networks has

been established. Conclusion of the paper is given in next section.

VI. Conclusions

In this research paper, we made efforts to overcome the challenge of security in mobile ad-hoc networks. This research paper presents a design and justification of a process calculi for secure ad-hoc network routing protocol. We designed *dRi* to formally model an Intrusion Detection System in Mobile Ad-hoc Networks in process algebraic framework. Implementation of the proposed language has been supported by detecting a malicious node in an example having simple mobile ad-hoc network consisting of six nodes. We justified this model *dRi* by showing that E-BUM is, in fact, top level view of *dRi* . Since E-BUM [19] is a specification for *dRi* therefore we have shown that *dRi* conforms to its specification. We will further verify this model using bisimulation based proof technique. The calculi developed is limited to stand-alone IDS which may further be extended to distributed IDSs.

References

[1] M. Alilou and M. Dehghant, "Upgrading performance of DSR routing protocol in mobile ad hoc networks," *Transactions on Engineering, Computing and Technology*, vol. 5, April 2005.

[2] M. Ilyas, *The Hand Book of Ad Hoc Wireless Network*, CRC Press LLC, 2003.

[3] P. Yadav and M. Gaur, "A survey on formal modelling for secure routing in mobile ad hoc networks," in *Proc. International Conference on Distributed Computing and Internet Technology*, 2015.

[4] H. Yang, H. Luo, F. Ye, S. Lu, and L. Zhang, "Security in mobile ad hoc networks," *Challenges and Solutions IEEE Wireless Communications*, February 2004

[5] W. Liu and Y. Fang, "SPREAD: Enhancing data confidentiality in mobile ad hoc networks," in *Proc. IEEE INFOCOM 2004*, 2004.

[6] Y. Hu, A. Perrig, and D. B. Johnson, "Packet leashes: A defense against wormhole attacks in wireless ad hoc networks," *Proc. IEEE INFOCOM 2003*, vol. 3, pp. 1976-1986, Apr. 2003.

[7] S. Buchegger and J. L. Boudec, "Performance analysis of the CONFIDANT protocol cooperation of nodes-fairness in dynamic ad-hoc networks," in *Proc. IEEE/ACM Symp. Mobile Ad Hoc Networking and Computing (MobiHOC)*, 2002.

[8] Y. Wang, G. Attebury, and B. Ramamurthy, "A survey of security issues in wireless sensor networks," *IEEE Commun. Surveys & Tutorials*, vol. 8, no. 2, Apr. 2006.

[9] Y. Hu and A. Perrig, "A survey of secure wireless ad hoc routing," *IEEE Computer Society*, 2004.

[10] Y. Hu and D. B. Johonson, "Securing quality-of-service route discovery in on-demand routing for ad hoc networks," *Proc. ACM SASN*, Oct. 20, 2004.

[11] X. Fei and W. Wang, "Modeling and analysis of connectivity in mobile ad hoc networks with misbehaving nodes," in *Proc. IEEE International Conference on Communications*, vol. 4, pp. 1879-1884, 2006.

[12] H. Lundgren, "Implementation and real-world evaluation of routing protocols for wireless ad hoc networks," Licentiate thesis, Uppsala University, 2002.

[13] H. Huttel. Willard Thor Rafnsson, Secrecy in Mobile Adhoc Networks. [Online]. Available: http://www.cse.chalmers.se/ rafnsson/article.pdf

[14] M. L. Pura, V. V. Patriciu, and I. Bica, "Modeling and formal verification of implicit ondemand secure ad hoc routing protocols in HLPSL and AVISPA," *International Journal of Computers and Communications*, vol. 3, no. 2, pp. 25-32, 2009.

[15] R. Chretien and S. Delaune, "Formal analysis of privacy for routing protocols in mobile ad hoc networks," in *Principles of Security and Trust*, 2013.

[16] X. Donghong1, J. Shujuan, and Q. Yong, "Security properties analysis of routing protocol for MANET," in *Proc. Second International Conference on Networks Security, Wireless Communications and Trusted Computing*, pp. 405-408, 2010.

[17] W. Mallouli, B. Wehbi, A. Cavalli, and S. Maag, "Formal supervision of mobile ad hoc networks for security flaws detection," in *Book chapter in Security Engineering Techniques and Solutions for Information Systems: Management and Implementation, Information Science Reference - IGI Global*, May 2011.

[18] A. Mishra, K. Nadkarni, and A. Patcha, "Intrusion detection in wireless ad hoc networks," *IEEE Wireless Communications*, vol. 11, no. 1, pp. 48-60, 2004.

[19] G. Lucia and S. Rossi, "A process calculus for energy-aware multicast communications of mobile ad hoc networks," *Wireless Communications and Mobile Computing*, vol. 13, no. 3, pp. 296-312, 2013.

Parul Yadav received the B.Tech. in Computer Science & Engineering from Dr. A.P.J. Abdul Kalam Technical University, Lucknow, Uttar Pradesh, India in 2005 and M.E. in Computer Science & Engineering and Information Technology from PEC University of Technology, Chandigarh, India in 2007. She is pursuing PhD in Computer Science from Institute of Engineering and Technology, Lucknow, Uttar Pradesh, India. Her research interests include Formal Modelling and Mobile Ad hoc Networks.

Manish Gaur received B.E. in Computer Engineering from S.V. Regional College of Engineering. and Technology, Surat, India in 1992 and M. Tech. in Computer Science and Engineering from Indian Institute of Technology Delhi (IIT Delhi), India in 2001. He is also PhD in Computer Science from Department of Informatics, University of Sussex,

UK and Post Doctorate from University of Glasgow, Scotland, UK. His research areas include Formal methods and verification of systems, Semantics of programming languages. Dr. Gaur is currently a Director at Centre of Advanced Studies, Lucknow.