An Agent Based Current Differential Relay for Use with a Utility Intranet

D. V. Coury
Member IEEE
Dept of Electrical Eng.
Engineering School of São Carlos
University of São Paulo
Brazil

J. S. Thorp
Fellow IEEE
School of Electrical Engineering
Cornell University
Ithaca, NY 14853
USA

K. M. Hopkinson
Student Member IEEE

K. P. Birman
ACM Fellow

Department of Computer Science
Cornell University
Ithaca, NY 14853
USA

Abstract: This paper proposes an agent-based current differential relay for use with a communication network. Agents are software processes capable of searching for information in networks, interacting with pieces of equipment and performing tasks on behalf of their owners (relays). Results illustrating the performance of the agent-based differential method proposed acting within a communication structure are presented for different traffic conditions. These results also show that a dedicated Utility Intranet is a viable and recommended option as a communication media for the proposed scheme.

Keywords: Differential Protection, Relaying, Transmission Lines, Agent Technology.

I.INTRODUCTION

Current differential relays are widely used for the efficient protection of buses, generators as well as power transformers. When applied to transmission lines, problems arise due to the distance between the line ends and consequently a communication channel is needed. The channels generally used for this purpose are power line carrier, microwave, communication cable or even fiber optics [1]. The differential technique relies on the fact that under normal conditions, the sum of the currents entering each phase of a transmission line from all connected terminals is equal to the charging current for that phase. If this sum exceeds a preset threshold, a fault may exist inside the protection zone.

Additional problems may arise due to synchronization of data between the two ends of the protected line when utilizing a digital communication link due to mismatched data sets [2]. Some recent publications concerning the digital differential protection of lines try to address these problems. Redfern et al [3] proposed a digital current differential protection using the limited data transfer capabilities of a digital data voice-frequency grade communication channel with satisfactory results. Li et al [4] proposed the Global Positioning Systems (GPS) for data synchronization. The results show a precise synchronized differential protection as well as the effect of current transformer saturation concerning the sensitivity of the protection.

This paper proposes an agent based differential relay for use with a Utility Intranet. Agents, as proposed in this paper, are software processes capable of searching for information in networks, interacting with pieces of equipment and performing tasks on behalf of their owners (relays). Moreover, they are autonomous and cooperative. Very few publications concerning the application of agents in the protection field have been reported in the literature. However, Tomita et al [5] proposed a cooperative protection system utilizing agents. Relay agents were constructed, and the cooperation of the main agents was simulated for primary, backup and adaptive protection. Coury et al [6] discuss the adaptation of the settings of distance relays for multi-terminal lines employing agents. It is shown that the digital relays and agents acting within a communication structure can alter adaptive settings to ensure correct performance over a wide variety of operation conditions.

Results illustrating the performance of the agent-based differential method proposed acting within a communication structure are presented in the following sections.

II.AGENT TECHNOLOGY

A software agent is a computer program that takes independent action based on events in the surrounding environment [7]. Under the control of some application that *owns* the agent, it is sent forth or placed at some site within a network where it takes local actions on behalf of its owners. Agents are dynamic entities. For example, an agent can exhibit dynamically changing behavior, receiving updated parameter settings from the owner or from other agents participating in the same application. An agent can also learn from the environment; the term "intelligent" is sometimes applied to such agents, particularly if the learning method involves artificial intelligence tools, or neural networks.

Agents can be further subdivided based on their mobility. *Mobile agents* can literally travel from one location to another while maintaining their state and functionality. One imagines such an agent as moving through a network in search of certain data, or for locations having certain attributes. In contrast, *local agents* are placed by the owner and then remain in the same location throughout their computational lives. Both kinds of agents normally have the ability to communicate with one another making mobility a lesser benefit than it might appear at first glance.

In the present paper, we consider the simplest kinds of agents: local, non-intelligent ones. Our work seeks to demonstrate advantages stemming from:

- The rapid response time made possible by placing a computational task close to the point where an action or measurement is needed.
- The simplicity of the power systems architecture afforded by the ability to send code to general purpose computing platforms.

The basic idea is that by doing so, new control paradigms can be introduced and executed efficiently, without changing the basic computing architecture of the power systems network.

The use of agents raises security considerations that go beyond those encountered in traditional software systems. Among the issues that need to be considered are the mechanism for installing agents and for communicating parameter updates to them, the means by which a computing platform or agent authenticates incoming messages, and the enforcement of agent resource restrictions, such as the use of scarce computational cycles or space in databases and file systems. Prior to deploying agents in mission-critical settings, one would need satisfying answers on all of these fronts. Preliminary work towards policies addressing these issues can be found in [8].

III. THE COMMUNICATION STRUCTURE AND THE POWER SYSTEM STUDIED

A. The communication structure

The computing infrastructure in which our agent community will operate is a subject of active speculation at the time of this writing. The existing power grid communication infrastructure is composed of a hodgepodge of equipment ranging from high-end fiber optic cables with large data bandwidth to crude systems with limited data transfer capabilities to nothing at all. Few utility communications lines are interconnected. However, this picture will change as utilities deploy ever more elaborate control mechanisms, demanding increasingly rich communication frameworks, steps that can easily be foreseen as part of the battle to improve operating efficiencies.

The relay scheme proposed here has modest network resource requirements compared to what we believe will be available in the near future. It is expected that the need for greater communication will result in a Utility Intranet (UI) that would interconnect control areas and their dependent entities using a relatively high capacity network similar to the Internet, but physically separate from it and dedicated to the power systems application. However, we caution that predictions of network bandwidth requirements and total network capacity can be deceptively reassuring. History has shown a tendency for networked applications to use all bandwidth made available to them.

To evaluate the feasibility of employing agents and network communication in power-systems relay protection, we need to understand the reliability and latency requirements of the relays. By doing so, we can determine whether or not a proposed combination of network hardware and communication protocols can meet the protection system's needs. Relays play a critical role in power grid operations with low tolerance for failures. One can identify that situations in communication between agents used for relay control might need to take place in as little as 10 ms, a latency realm leaving little time to recover from data transmission failures. It is therefore critical to ask whether available technology can meet those requirements.

The future Utility Intranet will certainly be built from off-the-shelf Internet-based technology. To do otherwise would be unreasonably costly both in terms of initial construction costs and the resulting maintenance requirements. Unfortunately, Internet routing hardware lacks any notion of service quality in network transmissions. Routers, as currently designed, drop information (packets) when load rises and do so even before congestion occurs. The approach makes sense for web browsers and email systems, but we need to ask what implication this behavior will have for power systems control. Within the Internet, all data delivery is executed on a "best-effort" basis without any possibility to raise the priority of one message over any other. In control applications, there are often situations where one needs to generate high priority events, and we should ask about the implications of running such applications over a network that lacks the corresponding capability.

These points raised earlier concerning priority suggest that power systems may need guarantees of “Quality of Service” (QoS). Unfortunately, while QoS has been a very active research topic for many years, there is such deep disagreement over the right approach to take (stemming from cost implications associated with most proposals) that no single solution has gained market acceptance, nor are standard solutions likely in the near future.

In order to face some of the network limitations, communication protocols like Cornell's Spinglass [9] have been developed. Spinglass allows the user to achieve high levels of reliability using protocols that probabilistically mask latency fluctuations and message loss. Spinglass could be optimized for use in power relaying and might form a powerful infrastructure for improved protection schemes.

B. The Network Simulator (NS)

This work uses NS (Network Simulator) [10] in its communication simulations. NS is a widely deployed network simulation testbed developed as part of a collaborative project between the University of California at Berkeley, Lawrence Berkeley Labs, the University of Southern California, and Xerox Parc under the Virtual Internetwork Testbed (VINT) project. NS has a large library of network protocols and the source code is designed for easy user-extensibility. Network topologies and traffic characteristics can be specified through the OTcl scripting language.

C. The Synchronization Problem

Synchronization of the transmitted signals is a very important step for the differential logic proposed. As mentioned before, synchronized measurement of power system quantities is possible using the Global Positioning System (GPS) [11]. This system was designed primarily for navigational purposes, but it furnishes a common-access timing pulse, which is accurate to within 1 microsecond at any location on earth [12]. The use of GPS receivers at each end on the protected line in order to guarantee sample synchronization is also proposed in this work. For the synchronization purpose, the transmitted samples must be time-tagged as illustrated by Fig. 1. As the transmitted signal is a complex number, the real and imaginary part of the samples is shown on the figure.

Samples		time
Re	**Im**	
1	1	1
.	.	.
.	.	.
N-2	N-2	N-2
N-1	N-1	N-1
N	N	N

Figure 1 Time-tagging process from the GPS signal

D. The Power System Utilized

In order to simulate the power system encountered in practice, this work also makes use of a digital simulator of faulted transmission lines known as PSCAD/EMTDC (Electromagnetic Transients and Controls Simulation Engine)[13]. It should be mentioned that although the technique described is based on Computer Aided Design (CAD), practical considerations such as the Capacitor Voltage Transformer (CVT), Current Transformer (CT) and anti-aliasing filters on system fault data were also included in the simulation. A 400 kV power system is shown in Fig. 2. The system consists of a tee configuration connected to a two-ended 100-km long transmission line 2-3, in which our studies will be concentrated. The agent based current differential relay for line 2-3 was also simulated.

IV. AGENT RELAYS

Fig. 3 presents the agent mechanism for protection purposes. It can be initially divided into a basic scheme for differential current calculation and additional features.

A. Basic Scheme for Current Differential Calculation

After passing through CVTs (Capacitive Voltage Transformers) and CTs (Current Transformers) in Fig. 3, the three phase voltage and current signals are digitized at 1.2 kHz. The proposed scheme is based on modal components of voltages and currents rather than phase values as the former has a number of distinct advantages over the latter. Modal components allows the three phase system to be treated like three single circuits independent of each other, thus simplifying the calculations considerably. The phase values are transformed into three modes: one Earth mode (1) and two Aerial modes (2,3) [14]. For the purpose of this work, only mode 2 was utilized, minimizing the need of transmitting three phase signals through the communication network as far as the differential logic is concerned. Perfect line transposition was assumed. This assumption does not add significantly to the inaccuracy of the scheme.

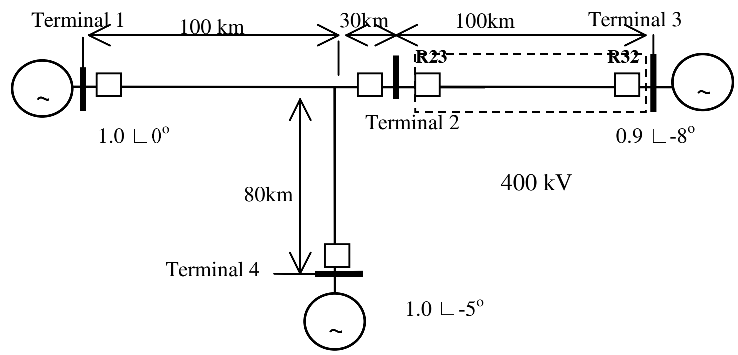


Figure 2 The power system utilized for tests

The next step considered in Fig. 3 was the use of one cycle Discrete Fourier Transform (DFT) in order to extract the 60 Hz component for mode 2 current and voltage at the line terminals. Following that, a line PI model is used for the shunt current compensation. Considering relay R32 this compensation is performed using equation (1):

$$\underline{I}_2' = C\underline{V}_3 + D\underline{I}_3 \tag{1}$$

where: V,I are mode 2 phasors, C,D are line constants

One of the novelties of the proposed method is the transmission of mode 2 current phasors instead of sampled values. In order to implement that, a one cycle moving window was utilized and the 60 Hz phasors (complex numbers) of I2' and I3' were transmitted through the network at a lower sample rate: 480 Hz. The great advantage of transmitting phasor values is that if samples are dropped in the transmission process, this will not invalidate the differential logic calculation at the two ends of the line. After re-sampling the signal at 480 Hz with the use of anti-aliasing filters, I3' and I2' are transmitted through the communication network in opposite directions and the differential logic is calculated at both ends of the line. In the case of an internal fault, circuit breakers associated to the agent relays will isolate the protected transmission line.

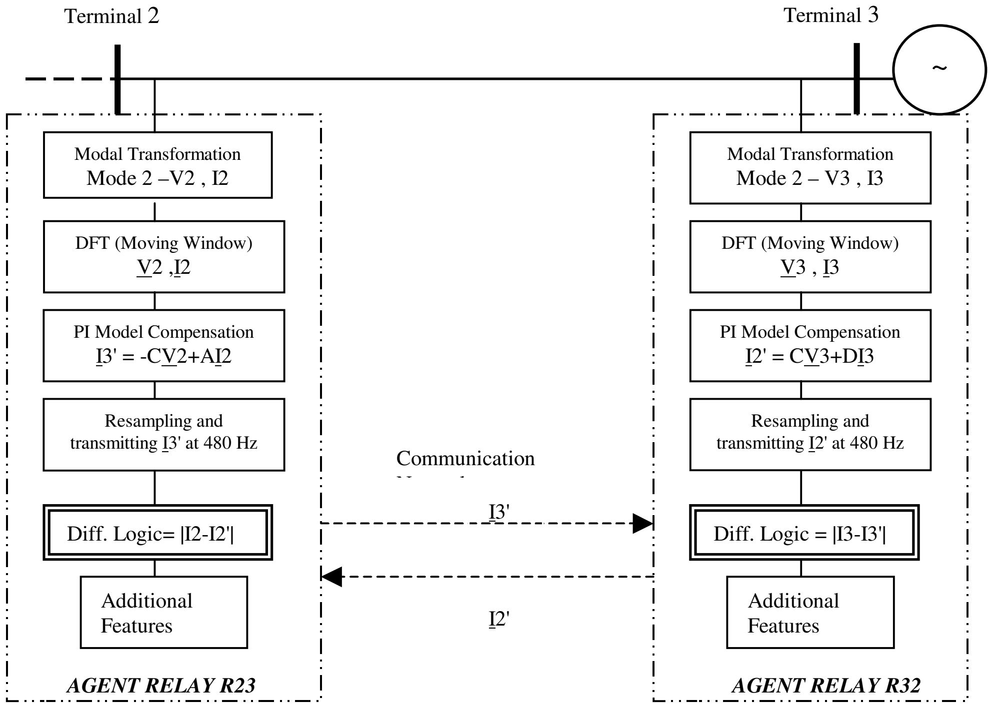


Figure 3 Agent mechanism for protection purposes

It should be mentioned at this point that a transient monitor was used in order to restrain the relay until the computed phasors are valid.

B. Additional Features

Some additional features for the agent-based relay are presented below:

- The scheme must work with a non-pilot agent protection simultaneously. The agent relays must constantly exchange information concerning the power system status, as well as equipment failure.
- The agent-based scheme must be able to detect equipment failure (CVTs, CTs, circuit breakers, etc) based on measurements. In the case of communication failure of local data, the agent-based relays must collect data from other pieces of equipment through the communication network. On the other hand, for a circuit breaker failure, a trip signal must be sent through the communication network to either local or remote ends in order to isolate a fault.
- The agent-based scheme must be able to detect communication channel failure as well as GPS signal failure. In the first case, a switch to non-pilot protection must be made (first item). In the second case, other ways of signal synchronization based on software must be implemented.

C. Discussion

One important issue concerns the advantages and disadvantages of using software agents in the proposed protection system, as opposed to employing some other more conventional means of signal processing and communication. For example, if existing architectures for control of regional power systems were simply moved to the Internet, or even a dedicated utility Intranet,one would arrive at a more centralized architecture, with a database system on some form of server. Data would be gathered from remote sensors and periodic control messages would be sent to the control systems, presumably using a standardized signaling protocol in which message formats, frequency of interaction, and other critical parameters were spelled out. Agents, in contrast, offer great flexibility but the very term evokes the troubling prospect of uncontrolled proliferation of control strategies and solutions. The resulting power system might be difficult to administer and perhaps even insecure and unreliable due to this flexibility.

Our use of agents in this paper should not be misinterpreted as a vote for chaos. We presume that before any sort of agent-based control system would be placed into widespread use, standards would be developed covering the following issues:

- Nature and permissible roles for agents.
- The management infrastructure associated with the agents.
- Standards for specific agent-based control paradigms considered appropriate for use in power systems.

We believe that any production-scale use of agents will demand the same degree of standardization and industry control as would a centralized control discipline. From this perspective, the remaining questions concern the technical advantages (or disadvantages) of representing emerging control paradigms using software agents, as opposed to some other architecture.

With these caveats, agents do bring some interesting and potentially valuable flexibility. Over time, one can predict that a number of new applications will be developed to take advantage of the Utility Intranet's potential. Additionally, agents offer the potential for sophisticated local monitoring policies. Rather than requiring that data be gathered at a central server, which then sends control actions back to the various control points, agents can potentially be programmed to do extensive local processing (where latencies are very low) and to take sophisticated actions. Because a single application creates and places the agents, one imagines such a solution as a form of distributed program, but one in which the computing happens "at the grassroots."

We are convinced that a flexible Utility Intranet communication architecture based on open standards is the best insurance against a never-ending series of incompatible system updates. The integrated computation and communication, that are the defining characteristics of agent technology, form an excellent foundation for a general approach to power systems solutions utilizing a Utility Intranet. When one wishes to add intelligence or other characteristics to an agent operation, it is easily done within the agent framework. Similarly, new communication protocols or application-level additions such as data stream compression can be implemented in agents without affecting the other portions of agent operations. New tasks can be added seamlessly by adding new agents to a system rather than modifying existing code. Mobility is also an easy extension to agent operation, if it is required. In short, agents are designed to operate at a level of abstraction that is both appropriate and compatible with a dynamic system like the developing utility communications infrastructure. The flexible nature of agents allows them to keep up with the expected growth of applications that take advantage of the Utility Intranet's potential.

Although this vision does imply the need for appropriate agent-oriented security mechanisms, management mechanisms, and standardization, all topics on which further research will be required, we are optimistic that no serious technical obstacles to success will arise. The hard problems involve identifying the best ways of mapping power systems control solutions to agent-based architectures, precisely the problem to which the experiments reported here are directed.

V. RESULTS OBTAINED

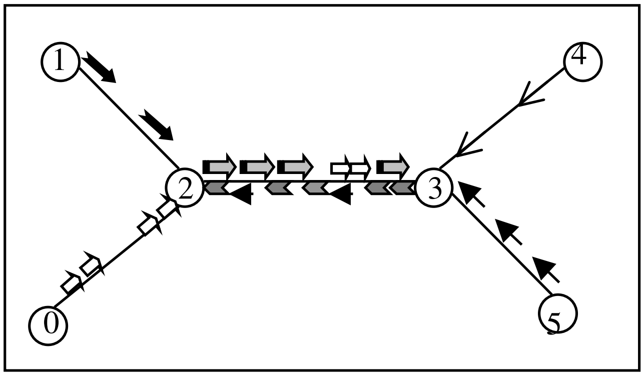
A. *The Use of the Network Simulator NS*

NS was utilized in order to simulate the transfer characteristic of the communication network. Fig. 4 illustrates the three relatively simple relay traffic scenarios created. The User Datagram Protocol (UDP) was selected as the transport protocol because relay measurements have a short useful lifetime and are also individually unimportant. The network topology used in our simulations was designed to reflect different levels of congestion that might be present in either the Internet or a dedicated Intranet without necessarily reflecting the same bandwidth or traffic flowing across such networks. The 1-2, 0-2, 4-3 and 5-3 links are designed to have a 5Mb capacity. The 2-3 link has a 1.6Mb capacity. All packet queues are *DropTail*, meaning that all new packets are dropped when a queue is filled to its capacity. The 2-3 link has a loss rate of 1% in either direction and no losses are simulated on the other links. Background traffic rates vary, but the phasor data exchange between nodes 2 and 3 for the considered agent-based relay happens at a constant rate of 480 Hz and with a constant data size of 52 bytes broken down into 20 bytes for the IPv4 header, 8 bytes for the UDP header, 16 bytes for the two double precision components of the phasor measurement (complex number), and an additional 8 bytes for the measurement's GPS timestamp. All scenarios begin at 1.0 second and end at 3.0 seconds. A representative subset of this sample is used in the agent based relay simulation presented in the next section. Two tables have been generated for each piece of traffic. One for the 3-2 traffic and another for the 2-3 information flow.

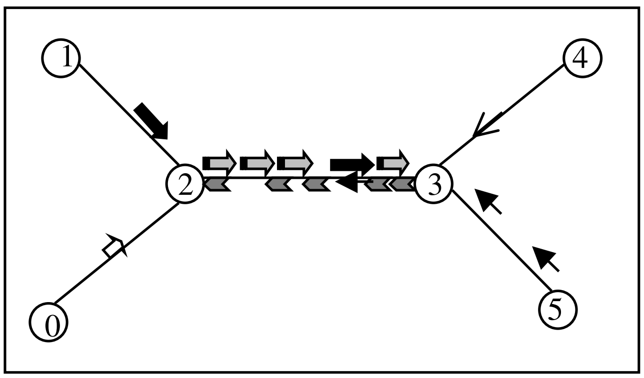
The heavy scenario was simulated based on Internet measurements taken in December 1999 and January 2000 and described in [15]. One of the conclusions that the authors made was that consecutive packets losses, known as loss runs, were 95% likely to occur in time intervals of 220 msec or less based on their empirical data. Considering the mentioned parameters, it is not difficult to conclude that the Internet is not suitable for relay communications. In order to simulate this scenario, constant traffic is sent from 0-3 and 5-2 at 2,000 samples per second (1024-byte) and from 1-3 and 4-2 at 833 samples per second (284-byte) and it is shown in Fig. 4(a). This results in a traffic flow that almost entirely overwhelms the relay traffic, as will be shown in the next section.

As mentioned earlier, the structure of the Utility Intranet is still speculative. There have been reports that substations will have 100 M bit Ethernet internally available to all power devices with fiber optic cable connecting substations and control centers together [16]. This level of Intranet bandwidth makes it entirely likely that relay traffic will always flow under lightly loaded conditions. The light scenario simulated consists of basic relay traffic between nodes 2-3 and 3-2 (Fig 4 (c)). There is no competing traffic so the only source of network losses comes from the basic 1% network loss rate.

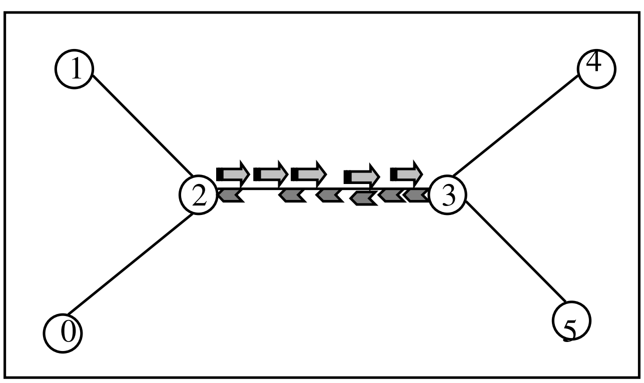
We have also constructed a scenario in between light and heavy to get a better idea of what a network with a background load that is neither overwhelming nor insignificant might look like (Fig. 4(b)). There is a constant 284-byte data stream from 1-3 and 5-2 at a rate of 333 Hz. There are also two 1024 byte data streams from 4-2 and 0-3 at a rate of 250 Hz. These background streams approach the bandwidth capacity of the 2-3 data link, but do not overwhelm the data queues. The result is a packet loss rate that varies from cycle to cycle, but is approximately 10% throughout the simulation.



(a) Heavy Scenario



(b) Medium Scenario



(c) Light Scenario

Figure 4 Transfer characteristics of the communication network considered in this study.

B. Results of the Agent Based Current Differential Relay

In order to test the proposed scheme, the agent-based current differential relay was simulated, acting with a communication network defined in the previous section. Tables 1, 2 and 3 show the behaviour of the proposed scheme for light, medium and heavy traffic in the communication network.

Table 1 shows the fault detection process for a three-phase internal fault occurring at 0.252 sec, 90 km from bus 2. It shows the differential current calculated by the relay when each new sample is available, the trip signal, as well as the transfer time for individual phasors considering light, medium and heavy traffic. The relay considered is located at bus 2, and the transfer times are related to transmitting the signal from terminal 3 to 2, through the communication network at 480 Hz, as mentioned before. '0' and '1' correspond to non-trip/trip conditions respectively. It should be mentioned that the shaded area in the tables relates to the use of the transient monitor, blocking the relay output during the first cycle after the fault.

Table 2 illustrates an external fault considering the transmission line 2-3. An a-to-earth fault is applied at 0.25 sec., 15 km from 2 in the tee configuration. As expected, the agent based relay does not detect such a fault. Again, different traffic conditions are presented.

Table 1 Detection process for a three-phase fault at 90 km (Incep. angle = 45^o; Rf=100 ohms, fault instant= 0.252 msec,)

Time (sec)	**Idiff (Re) kA*10**	**Idiff (Im) kA*10**	**Trip**	**Trans-fer time msec Light Traff.**	**Trans-fer time msec Medium Traff.**	**Trans-fer time msec heavy Traff.**
0.24575	0.0046	0.088	0	6.04	24.29	-
0.24783	0.0050	0.089	0	6.05	24.55	-
0.24991	0.0056	0.089	0	5.26	-	-
0.25200	0.0055	0.088	0	5.52	24.82	-
0.25408	0.0049	0.088	0	5.78	25.08	-
0.25616	-0.47	2.10	1	6.04	25.34	-
0.25825	4.11	11.81	1	6.05	-	-
0.26033	19.41	17.83	1	5.26	-	-
0.26241	32.04	12.77	1	5.52	24.57	-
0.26450	33.71	10.08	1	5.78	24.83	-
0.26658	37.73	18.24	1	6.04	25.09	-
0.26866	52.56	24.04	1	6.05	25.35	-
0.27075	65.02	19.04	1	5.26	25.36	-
0.27283	67.15	14.40	1	5.52	24.59	-
0.27491	66.60	12.89	1	5.78	24.85	-
0.27700	66.33	12.72	1	6.04	25.11	-
0.27908	66.07	12.71	1	6.05	25.37	-
0.28116	66.01	12.77	1	5.26	25.38	-
0.28325	66.01	12.81	1	5.52	24.60	-
0.28533	66.04	12.83	1	5.78	24.86	-
Diff. Relay Detection Time(msec)				***24.01***	***44.11***	***178.9***

Table 2 Differential process for an external fault at 15 km (a-to-earth fault, Incep. angle = 0^o; Rf=10 ohms, fault instant=0.25 sec)

Time (sec)	Idiff (Re) kA*10	Idiff (Im) kA*10	Trip	Trans-fer time msec Light Traff.	Trans-fer time msec Medium Traff.	Trans-fer time msec heavy Traff.
0.24375	0.00505	0.0887	0	6.04	24.23	-
0.24583	0.00460	0.0892	0	6.05	24.49	-
0.24791	0.00504	0.0897	0	5.26	24.50	-
0.25000	0.00561	0.0894	0	5.52	24.78	-
0.25208	0.00556	0.0890	0	5.78	25.04	-
0.25416	0.00316	0.0858	0	6.04	25.30	-
0.25625	-0.0059	0.065	0	6.05	-	-
0.25833	-0.036	0.0451	0	5.26	-	-
0.26041	-0.079	0.044	0	5.52	24.52	-
0.26250	-0.119	0.064	0	5.78	-	54.22
0.26458	-0.143	0.099	0	6.04	-	-
0.26666	-0.144	0.133	0	6.05	-	-
0.26875	-0.116	0.150	0	5.26	-	-
0.27083	-0.115	0.145	0	5.52	24.80	-
0.27291	-0.112	0.147	0	5.78	25.06	53.44
0.27500	-0.108	0.152	0	6.04	25.32	-
0.27708	-0.102	0.153	0	6.05	25.58	-
0.27916	-0.102	0.152	0	5.26	25.59	-
0.28125	-0.098	0.146	0	5.52	23.77	-
0.28333	-0.098	0.139	0	5.78	24.03	-
Diff. Relay Detection Time (msec)				**-**	**-**	**-**

Table 3 Detection time for a differential protection scheme (transfer frequency= 480 Hz) for various conditions considering light, medium and heavy traffic scenarios.

Fault Dist. (km)	Fault Type	Ince pAng le (^{o})	Fault Resi stan ce (Ω)	Detection Time msec Light Traff.	Detection Time msec Medium Traff.	Detection Time msec Heavy Traff.
10	AG	0	10	24.01	44.33	78.80
10	BC	0	10	24.01	41.47	295.36
10	BCG	0	10	24.02	43.02	306.45
10	ABC	0	10	24.01	42.94	88.27
50	BG	90	50	23.90	45.08	94.32
50	BA	90	50	24.80	45.39	74.04
50	BAG	90	50	24.80	43.88	196.16
50	ABC	90	50	24.27	41.55	85.04
90	CG	45	100	24.01	42.12	75.98
90	AC	45	100	24.79	43.23	242.46
90	ACG	45	100	24.01	43.55	76.35

Finally, Table 3 shows the performance of the proposed scheme in terms of detection time for various internal faults, once more considering light, medium and heavy traffic. Some of the parameters that were varied are fault distance and type, inception angle as well as fault resistance. In all tables there is an exceptionally long detection time for heavy traffic conditions. In some cases the detection time for such a situation was almost 19 cycles, making that totally incompatible with the relay needs. Light and Medium traffic presented detection times of about 1.5 and 2.5 cycles after the fault occurrence, respectively. These results show that a dedicated Utility Intranet is a viable and recommended option as a communication media for the proposed scheme.

VI. CONCLUSION

This paper presented an application of an agent-based current differential relay for use with a communication network. Results illustrating the performance of the new proposed method considering different traffic characteristics for the communication network were presented.

It can be concluded that the new method based on agent technology offers some additional features. Equipment failure detection, the ability to transfer trips via the communication network, and the capability to collect data from any point of the power system are all notable improvements offered by our approach. Our proposed method can also be seen as an illustration of the way that relays can use a communication network in order to receive greatly clarified views of the state of the surrounding power system.

We considered light, medium, and heavy network traffic scenarios. We learned that it would be impractical to use the Internet for time-sensitive relay protection communications. A dedicated Utility Intranet with adequate bandwidth could provide the necessary traffic delivery and data transfer levels while simultaneously facilitating potential communication between devices located anywhere within the electric power grid.

VII . ACKNOWLEDGMENTS

The authors acknowledge the research support by subcontract No. 35352-6085 with Cornell University under WO 8333-04 from the Electric Power Institute and the U.S. Army Research Office as well as FAPESP (Fundação de Amparo à Pesquisa do Estado de São Paulo -Brazil).

VIII. REFERENCES

[1] S.H. Horowitz and A.G. Phadke, Power System Relaying, John Wiley and Sons, 1996.

[2] W.S. Kwong, "Current Differential Protection Goes Digital" Journal of Modern Power Systems, January 1988, pp. 53-56.

[3] M.A. Redfern, A.A.W. Chiwaya "A New Approach to Digital Current Differential Protection for Low and Medium Voltage Feeder Circuit using a Digital Voice-Frequency Grade Communication Channel", IEEE Transaction on Power Delivery, vol.9, no 3, July 1994, pp. 1352-1358.

[4] H.Y. Li, E.P. Southern, P.A. Crossley, S. Potts, S.D.A. Pickering, B.R.J. Caunce, G.C. Weller "A New Type of Differential Feeder Relay Using the Global Positioning System for Data Synchronization", IEEE Transactions on Power Delivery, Vol. 12, no 3, July 1997, pp. 1090-1097.

[5] Y. Tomita, C. Fukui, H. Kudo, J. Koda, K. Yabe, “A Cooperative Protection System with an Agent Model”, IEEE Transactions on Power Delivery, Vol.13, n^o 4, October 1998, pp. 1060- 66.

[6] D.V.Coury, J.S. Thorp, K.M. Hopkinson, K.P. Birman "Agent Technology Applied to Adaptive Relay Setting for Multi-Terminal Lines", IEEE PES Summer Meeting, Seattle, July 2000.
[7] M. Genesereth and S. Ketchpel, "Software Agents", Communications of the ACM, Vol. 37, n. 7, July 1994, pp. 48-52.
[8] F. Schneider, "Towards Fault-tolerant and Secure Agentry", Proceedings 111th International Workshop on Distributed Algorithms, Lecture Notes in Computer Science, Volume 1320, September 1997, pp. 1-14.
[9] K. Birman, M. Hayden, O. Ozkasap, Z. Xiao, M. Budiu and Y. Minsky "Bimodal Multicast" ACM Transactions on Computer Systems, Vol. 17, No. 2, May 1999.
[10]UCB/LBNL/VINT Network Simulator – NS- version 2 (http://www-mash.cs.berkeley.edu/ns/)
[11] Working Group H-7, "Synchronized Sampling and Phasor Measurement for Relaying and Control", IEEE Trans. on Power Delivery, Vol. 9, no 1, Jan. 1994, pp. 405-412.
[12] A.G. Phadke, "Synchronized Phasor Measurements in Power Systems", IEEE Computer Applications in Power, April 1993.
[13] PSCAD/EMTDC Manual, Getting Started, Manitoba HVDC Center 1998
[14]L.M. Whedepol, "Application of Matrix Methods to the Solution of Travelling-Wave Phenomena in Poly-Phase Systems", Proc. IEE, 1963, 110, (12), pp. 2200-2212.
[15] Y Zhang, V. Paxson, S. Shenker, "The Stationarity of Internet Path Properties: Routing, Loss, and Throughput". ACIRI Technical Report, May 2000.
[16] EPRI Report, "Test Methodologies, Setup, and Result Documentation for EPRI Sponsored Benchmark of Ethernet for Protection Control", Version 1.0, May 12, 1997.
Available at ftp://www.sisconet.com/epri/benchmrk/ethernet.zip

IX. BIOGRAPHIES

Denis V. Coury was born in Brazil, in 1960. He received a B.Sc. degree in Electrical Engineering from the Federal University of Uberlandia, Brazil in 1983, a MSc degree from the University of São Paulo, Brazil in 1986 and a Ph.D. degree from Bath University, England in 1992. He joined the Department of Electrical Engineering, University of São Paulo, São Carlos, Brazil in 1986, where he is an Associate Professor in the Power Systems Group. He spent his Sabbatical at Cornell University in 2000. His areas of research interest are Power System Protection as well as new techniques for Power System Control and Protection including the use of Expert Systems and Artificial Neural Networks. Email coury@sel.eesc.sc.usp.br

James S. Thorp is the Charles N. Mellowes Professor in Engineering and Director of the School of Electrical Engineering at Cornell University. In 1976, he was a faculty intern at the AEP Service Corporation. He was an associate editor for IEEE Transactions on Circuits and Systems from 1985 to 1987. In 1988, he was an overseas fellow at Churchill College, Cambridge, England. He is a member of the National Academy of Engineering, a Fellow of IEEE and a member of the IEEE Power System Relaying Committee, CIGRE, Eta Kappa Nu, Tau Beta Pi and Sigma Xi. Email jst6@cornell.edu

Kenneth M. Hopkinson is a native of Charlotte, North Carolina. He received his BS degree in Computer Science from Rensselaer Polytechnic Institute in 1997. Since that time, Ken has been working towards his Ph.D. degree in Computer Science at Cornell University in Kenneth Birman's Ensemble research group. His areas of interest include distributed computer systems and network communications protocols. Ken Hopkinson is currently investigating communications issues arising in the power grid under deregulation. Email hopkik@cs.cornell.edu

Kenneth P. Birman is a Professor of Computer Science at Cornell University. A Fellow of the ACM, Birman has published extensively on reliable, secure distributed computing since joining Cornell in 1982. He developed the Isis Toolkit, which controls communication in the New York Stock and Swiss Exchanges, the French air traffic control system, and oversaw development of Cornell's Horus, Ensemble and Spinglass systems. He was Editor in Chief of ACM Transactions on Computer Systems from 1994-1999. He has advised the government on hardening the nationally critical communications infrastructure, and was co-chair of the 1995 DARPA ISAT study that set the research agenda in this field. Email ken@cs.cornell.edu